Networking your world

NS-2024E

24+2G HYPER CONNECT MANAGED SWITCH

USER'S MANUAL

Http://www.netsys.com.tw

Copyright

Copyright © 2011 by National Enhance Technology Corp. All rights reserved.

Trademarks

NETSYS is a trademark of National Enhance Technology Corp.
Other brand and product names are registered trademarks or trademarks of their respective holders.

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, National Enhance Technology Corp. hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETSYS reserves the right to make changes to the products described in this document without notice. NETSYS does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Maximum signal rate derived from IEEE Standard specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Netsys does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Make sure you follow in line with the environmental conditions to use this product.

Gigabit Ethernet Switch features

The NS-2024E Intelligent Ethernet Switch supports 24 x 10/100M Ports(RJ45)，2x1000Mbps RJ-45(Copper media) or SFP support auto-link and hot swapping function) It is an one rack-unit (1RU) high, 14-inches deep. It is a standard 19" Rack mounted size.

The NS-2024E Intelligent Ethernet Switch provides the important features necessary for robust networks:

- **Quality of Service**: 802.1p QOS supports. Provides high-and low-priority queuing on a per-port basis.
- **IGMP** Snooping by 256 IP multicast table for VOD (Video on demand) and Video conference and Internet games application
- **Scalability**: Up to **100** Mbps symmetric performance over CAT 5 cable Fast Ethernet Channel port aggregation.
- **Security**: **802.1Q** Q-in-Q/Multiple VLAN and **port-based** virtual local-area network (VLAN) support. Private VLAN access, assuring port security without requiring a VLAN per port, and also **Supports MAC filtering to Lock MAC address.**
- **In band Management :** Provides a console port for setup IP or other function
- **Out Of Band Management:** Supports remote control by Telnet and Web-based Management easy-to-use configuration and ongoing monitoring. This software is embedded in the switch and delivers remote, intuitive management of the switch and connected NIC devices through a single IP address. The 24+2G Intelligent Ethernet Switch are easy-to-configured and deployed, and offering a compelling option in terms of cost, performance, scalability and services compared to traditional repeater HUB solutions.
- **Speed Rate Control:** Supports speed rate control function from 128k to 100Mbps.

Note:

Regarding NS-2024E bandwidth control, which must rely on flow control to limit bandwidth, therefore if client side doesn't support flow control, upstream bandwidth control will invalid, so for this case, client side must support flow control function.

- **IEEE-802.1x:** port base network access control, this function for wireless users connecting Authentication.
- **Spanning tree:** Supports IEEE802.1d for MAC bridge and link redundant.
- **Port Mirroring:** This function could be mirroring and duplicated client side action, but Need to be with mirroring AP as

Session wall or other

- **DHCP Client:** Dynamic Host Configuration Protocol (DHCP) for auto configure management IP.
- **TFTP Protocol:** Trivial File Transfer Protocol(TFTP) for new version firmware remote upgraded.
- **SNMP MIB Support:** SNMP v1/v2c/v3 management and trap function

  Support MIB tables: MIB-II (RFC 1213), Bridge MIBs (RFC 1493), Ethernet-like MIB (RFC 1643 & RFC 2665), private-MIB, USM-MIB (RFC 2574), VACM-MIB (RFC 2575) and RMON-MIB 1, 2, 3, 9 groups (RFC 1757& RFC 2819)
- **HTTPS (SSL) Web Access:** Supports secured web-based management.
- **Giga port auto link supports:** This function can be auto sensing client interface media with Copper or fiber optic and link one and supports hot swap.

Attention:

Be sure to read this manual carefully before using this product. Especially Legal Disclaimer, Statement of Conditions and Safety Warnings.

Caution:

The NS-2024E is for **indoor** applications only. This product does not have waterproof protection, please do not use in outdoor applications.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions before using the device.

- **DO NOT** open the device or unit. Opening or removing the cover may expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- **Use ONLY** the dedicated power supply for your device. Connect the power to the right supply voltage (110V AC used for North America and 230V AC used for Europe).
- **Place** connecting cables carefully so that no one will step on them or stumble over them. DO NOT allow anything to rest on the power cord and do NOT locate the product where anyone can work on the power cord.
- **DO NOT** install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- **DO NOT** expose your device to dampness, dust or corrosive liquids.
- **DO NOT** use this product near water, for example, in a wet basement or near a swimming pool.
- **Connect ONLY** suitable accessories to the device.
- **Make sure** to connect the cables to the correct ports.
- **DO NOT** obstruct the device ventilation slots, as insufficient air flow may harm your device.
- **DO NOT** place items on the device.
- **DO NOT** use the device for outdoor applications directly, and make sure all the connections are indoors or have waterproof protection place.
- **Be careful** when unplugging the power, because it may produce sparks.
- **Keep** the device and all its parts and accessories out of the reach of children.
- **Clean** the device using a soft and dry cloth rather than liquid or atomizers. Power off the equipment before cleaning it.
- This product is **recyclable**. Dispose of it properly.

Table of Contents

Copyright 1
Gigabit Ethernet Switch 2
Safety Warnings 4
Chapter 1. Unpacking Information 8
Check list 8
Product Guide 9
Chapter 2. General Description 12
Hardware Description 12
Front Panel 12
SFP Fiber Optics 14
LED Indications 15
Rear Panel 16
AC Power Socket 16
Chapter 3. Installation 17
Hardware Installation 17
Pre-Installation Requirements 17
General Rules 18
Connection Configuration 18
Chapter 4. Management Configuration 20

4.0 In-Band Management 20
4.1 Remote Network Management 26
4.1.1 IP Setting 27
4.2 Administration 30
4.2.1 IP Address Setting 31
4.2.2 Switch Setting 32
4.2.3 Console Port Information 36
4.2.4 Port Configuration 37
4.2.5 SNMP Configuration 43
4.2.6 Syslog 49
4.2.8 Configuration Backup 53
4.3 L2 Features 55
4.3.1 VLAN Configuration 55
4.3.2 Trunking 67
4.3.3 Forwarding and Filtering 74
4.3.4 Spanning Tree 82
4.3.5 DHCP Relay and Option 82 98
4.3.6 LLDP 100
4.4 Access Control List 103
4.4.1 IPv4 105
4.4.2 Non-IPv4 109
4.4.3 Binding 111
4.4.4 QoS VoIP 113
4.5 Security 115

4.5.1 Security Manager 115
4.5.2 MAC Limit 116
4.5.3 802.1x Configuration 118
4.6 QoS 123
4.6.1 QoS Configuration 123
4.6.2 Per-Port Configuration 125
4.7 Monitoring 127
4.7.1 Port Status 127
4.7.2 Port Statistics 128
4.8 Reset System 129
4.9 Reboot 129
Chapter 5. Applications 130
Appendix A: Troubleshooting 134
Diagnosing Switch Indicators 134
System Diagnosis 137
System Integrity 138
Warranty 140
Chinese SJ/T 11364-2006 141

Chapter 1. Unpacking Information

Check list

Carefully unpack the package and check its contents against the checklist.

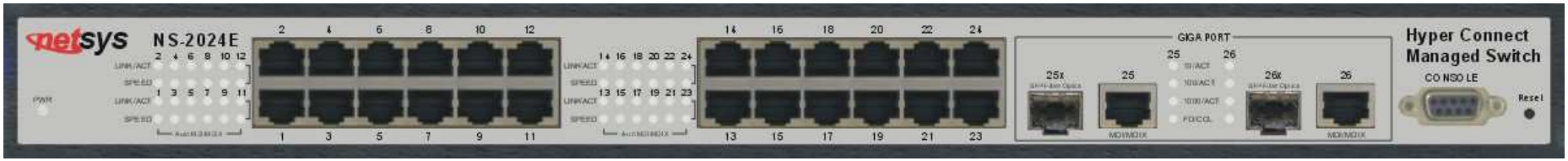
Package Contents

- 1 x NS-2024E (Intelligent Ethernet Switch)
- 1 x AC Power Cord
- 1 x Accessory Kit : 2 x Rack Mounting Brackets, 4 x Screws

Notes:

1. Please inform your dealer immediately for any missing or damaged parts. If possible, retain the carton including the original packing materials. Use them to repack the unit in case there is a need to return for repair.
2. If the product has any issue, please contact your local vendor.
3. Please look for the QR code on the bottom of the product, the user can launch the QR code scanning program to scan and download the user's manual electronic format file.

Product Guide



Product Name：2 ports 1000 Mbps Ethernet plus 24 ports 10/100 Mbps with SNMP Management Switch

Key Features:

- Provides 2 x 10/100/1000Mbps auto-sensing RJ-45(Copper mode) or SFP Auto-link and Hot Swap Ethernet ports for connects trunking.
- Support Copper/ Fiber Auto-Link with hot swap for Gigabit Ethernet port.
- Support Jumbo packet up to 9k bytes.
- Support bandwidth management(rate control).
- Support IEEE 802.1q tagging VLAN with Q-in-Q.
- Support QOS IEEE-802.1p with 4 priority queues.
- Support HTTPS (SSL) web management.
- Support Multicast IP table/IGMP v2 with 512 groups.
- Support LACP IEEE-802.3ad port trunking (link aggregation).
- Support IEEE 802.1d STP / IEEE 802.1w RSTP & IEEE-802.1s MSTP.
- Support port mirroring (sniffer) and broadcast storm filtering.
- Support port security with MAC address filtering.
- Support remote syslog and traffic storm control.
- Support IEEE 802.1x Access Control Improve Network Security

- Support Web based and telnet for remote management.
- Support SNMP v1/v2/v3 RFC-1493 bridge MIBs, RFC-1643 Ethernet MIB, RFC-1213 MIBII.
- Support RMON groups 1(Statistics), 2(Alarm), 3(Event), 9(History).
- Support HTTP/TFTP for firmware upgrade.
- Support console management.
- Support L2/L3/L4 access control list(ACL).
- Support DHCP client and Relay & Option 82.
- Support LLDP(Link Layer Discovery Protocol) protocol.
- EMI certified by FCC, CE

Specifications:

Standard:	IEEE802.3 standard
	IEEE802.3u standard
	IEEE802.3z standard
	IEEE802.3ab standard
Interface:	24 x RJ-45 10/100Mbps Ethernet port
	2 x RJ-45/SFP 10/100/1000Mbps connector
Flow control:	Full duplex: IEEE 802.3x
	Half duplex: Back pressure
MAC address table:	8K Entries
LED indication:	Power
	Link/Active/Speed/Duplex Status for Ethernet port
Internal switching power adapter Input:	AC 85-265 volts/50-60Hz/1A
Power Consumption:	22W
Operating Temperature:	0°C ~ 50°C (32°F ~ 122°F)
Storage Temperature:	-20°C ~ 65°C (-4°F ~ 149°F)
Humidity:	10 to 90% (non-condensing)
Dimensions:	443.6 x 215 x 44 mm

Chapter 2. General Description

Hardware Description

This section describes the important parts of the switch. It features the front and rear panel drawings LEDs, connectors, and switches.

Front Panel

The following figure shows the front panel.(Figure 2.1)

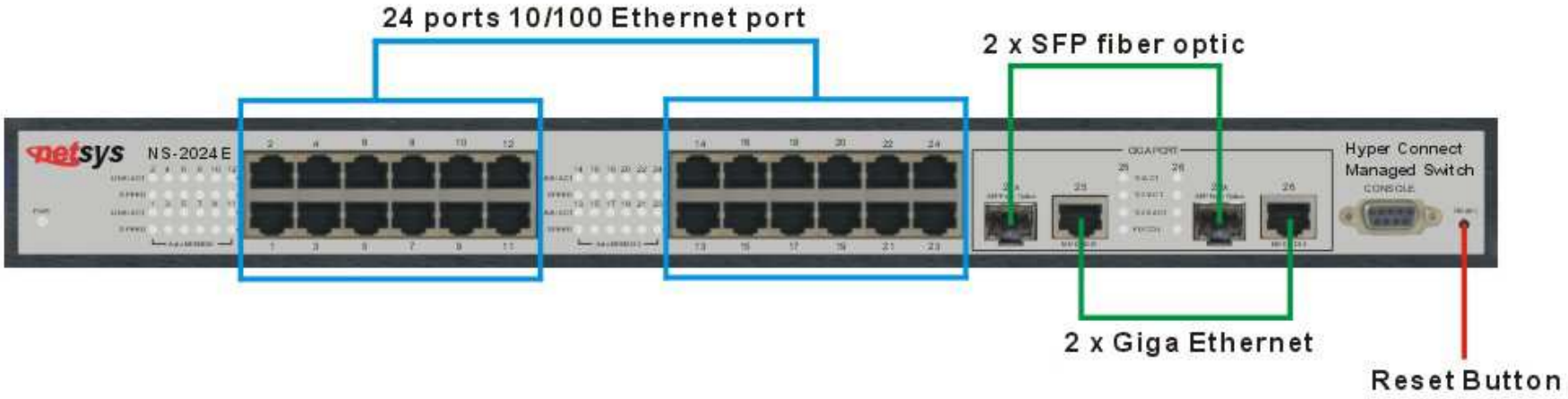


Figure 2.1 Front Panel description

(1) "PWR.": Power LED light.

(2) 24 x 10/100Mbps auto sensing RJ-45 Ethernet ports

(3) 2 x 1 Giga auto link RJ-45 or SFP Transceivers.

(4) Console port (RS-232)
(5) Reset Button.

Several LED indicators for monitoring the device itself, and the network status. At a quick glance of the front panel, the user would be knew if the product is receiving power; if it is monitoring another switch or other devices; or if a problem exists on the network.

Provide two 1000Mbps auto-sensing RJ-45 Ethernet ports and two GIGA Port.
GIGA Port supports RJ-45 or SFP Interface auto link function. You can use RJ-45 interface or SFP

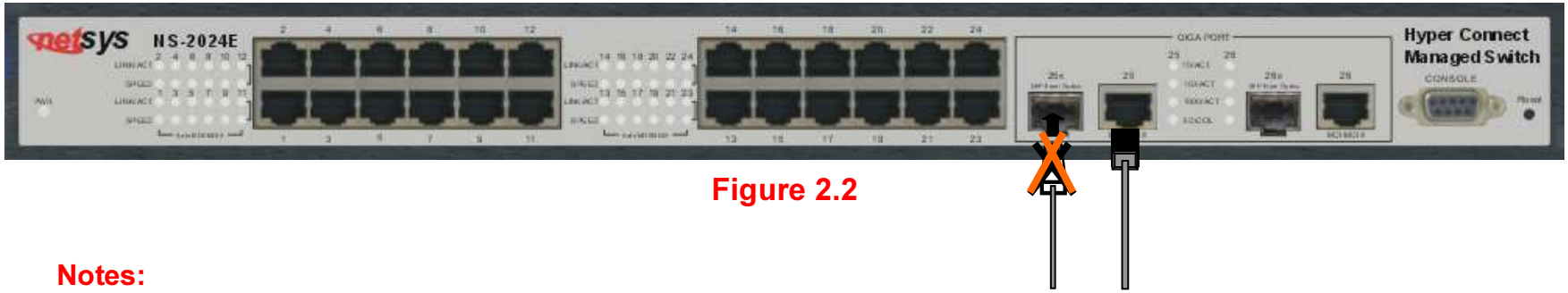


Figure 2.2

Notes:

NS-2024E supports two gigabit TP/SFP combo interfaces, one is copper interface and the other is small fiber optic interface. 25 and 26 port is RJ45 interface, 25x and 26x port is SFP interface. GIGA port supports Hot Swappable function; user can plug or unplug Giga port when the switch is operating. Please note that do not use the GIGA port RJ-45 interface and SFP interface in the same time, otherwise it will link in Copper mode (default).

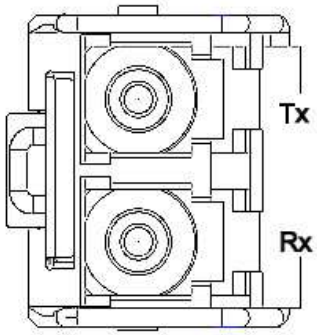
SFP Fiber Optics

A gigabit interface converter (SFP) is a transceiver that converts electric currents (digital highs and lows) to optical signals, and optical signals to digital electric currents. The SFP is typically employed in fiber optic and Ethernet systems as an interface for high-speed networking. The data transfer rate is 1.25 gigabit per second.

SFP modules allow technicians to easily configure and upgrade electro-optical communications networks. The typical SFP transceiver is a plug-in module that supports hot-plugging (it can be removed and replaced without turning off the system). The devices are economical, because they eliminate the necessity for replacing entire boards at the system level. Upgrading can be done with any number of units at a time, from an individual module to all the modules in a system. SFP (Small Form Pluggable Transceivers), meet the Gigabit Interface Converter specification Rev. 5.4 (MOD_DEF4) industry standard.

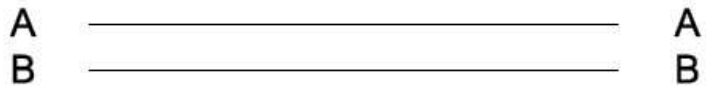
	Mode	Wave length	Bit Rate	Voltage	Power Margin
1	LX-Single Mode	10km	1.25Gbps	3.3V	10.5db(10KM or above)
2	SX- Multi Mode	550m	1.25Gbps	3.3V	8.5db(550m)

Pinouts



Cable Wiring

Cable Wiring



LED Indications

Table 2-1 LED Indicators Description and Operation

LEDs	Color	Status	Descriptions
PWR (Power LED)	Green	ON	This LED light is located at the left side on the front panel. It will light up (On) to show that the product is receiving power. In contrast, no light (Off) means that the product has no power.
		OFF	
Link / ACT (1-24) (Receiving LEDs)	Green	Steady	LED is lit up steady to show "Link".
		Blinking	Blinking to show data on Receiving status
Speed (1-24) Speed LEDs	Green	Steady	Indicates that communications have been set 100 Mbps. Each port on the switch is assigned an LED light for 100 Base-TX connecting.
10 LINK/ACT (Giga Port LED)	Green	Steady	Each RJ45 station port on the Ethernet is assigned an LED light for "**10M** Good Linkage". Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage.
		Blinking	Giga port Act LED if Blinking to show data on Receiving status
100 LINK/ACT (Giga Port LED)	Green	Steady	Each RJ45 station port on the Ethernet is assigned an LED light for "**100M** Good Linkage". Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage.
		Blinking	Giga port Act LED if Blinking to show data on Receiving status
1000 LINK/ACT (Giga Port LED)	Green	Steady	Each RJ45 station port on the Ethernet is assigned an LED light for "**1000M** Good Linkage". Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage.
		Blinking	Giga port Act LED if Blinking to show data on Receiving status

LEDs	Color	Status	Descriptions
FD/COL (Full-Duplex LED) (Collision LED) (Giga Port LED)	Green	Steady	Indicates that communications have been set to full-duplex operation for the indicated port, and light down working in Half Duplex
		Blinking	Blinking to show collision status.

Rear Panel

The following figure shows the rear panel of the switch

Figure 2.3 Rear Panel

AC Power Socket

The power cord should be plug into this socket. The AC Socket accepts AC power 100 to 240 voltage.

Chapter 3. Installation

Hardware Installation

This chapter describes how to install the Switch and establish network connections. You may install this Switch on any level surface (table, shelf, 19 inch rack or wall mounting). However, please take note of the following minimum site requirements before you begin. **NS-2024E pre-installed 4 plastic feet.**

Pre-Installation Requirements

Before you start actual hardware installation, make sure you can provide the right operating environment, including power requirements, sufficient physical space, and proximity to other network devices that are to be connected. Verify the following installation requirement:

- Power requirements: AC 100V to 240 V at 50 to 60 Hz.
  The Switch power supply automatically adjusts to the input voltage level.
- The Switch should be located in a cool dry place, with at least 10cm/4in of space at the front and back for well ventilation.
- Place the Switch away from **direct sunlight**, **heat sources**, or areas with a high amount of electromagnetic interference.
- Check if network cables and connectors needed for installation are available.

General Rules

Before making any connections to the modem, take note the following rules:

Ethernet Port (RJ-45)

- All network connections to the Switch Ethernet port must be made using Category 5e-7 UTP/STP for 10/100/1000Mbps, Category 5 UTP/STP for 10/100Mbps and Category 3,4 UTP for 10Mbps.
- No more than 100 meters (about 328 feet) of cabling may be used between the Switch and an end node.

Connection Configuration

The Switch has 24 10/100 Mbps N-way ports and two force 1000Mbps ports which support connection to 10Base-T Ethernet or 100Base-TX Fast Ethernet. Support full or half-duplex operation and Auto MDI/MDIX. The transmission mode is using auto-negotiation. Therefore, the devices attached to these ports must support auto-negotiation unless they will always operate at half duplex. If transmissions must run at full duplex, but the attached device does not support auto-negotiation, then you should upgrade this device to a newer version that supports auto-negotiation.

Use any of the 1~26 ports to connect to devices such as a workstation, server, bridge or router. You can also cascade to another compatible switch or hub by connecting an MDI or MDIX port.

1. You can connect (1~24) station port on the switch to any device that uses a standard network interface such as a Cable modem, ADSL modem workstation or server, or also to a network interconnection device such as a bridge or router (depending on the port type implemented).

2. Prepare the network devices you wish to network. Make sure you have to install suitable 10BASE-T or 100BASE-TX network interface cards before making a connection to any of the Ethernet switch (1~24) station ports. You also need to prepare 100Ω Category 5 straight-through shielded or unshielded twisted-pair cables with RJ-45 plugs at both ends.
3. Connect one end of the cable to the RJ-45 port of the network interface card, and the other end to any available (1~24)

station port on the switching. Every port support either 10 or 100 Mbps connections. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. Using the switch in a stand-alone configuration, you can network up to 24 nodes.

Notes:

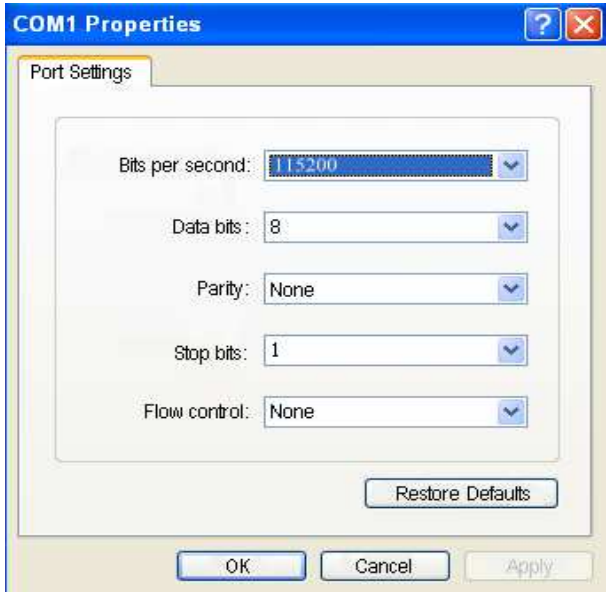
1. Please note that each twisted-pair cable (RJ-45) does not exceed 100 meters (328 feet).
2. We recommend use Category 5~7 cable to connect Ethernet device to avoid any confusion or inconvenience.

Chapter 4. Management Configuration

4.0 In-Band Management

Console port (RS-232) Configuration (Change IP Address via Hyper Terminal)

User can configure the product with the local serial console port, if one of the Ethernet port is not in use, you can disable it, that procedure is to connect a notebook computer to the RS-232 port, then boot operating systems, such as using the Windows operating system, and run "Hyper-terminal" program into terminal window, and setup step are as follow.



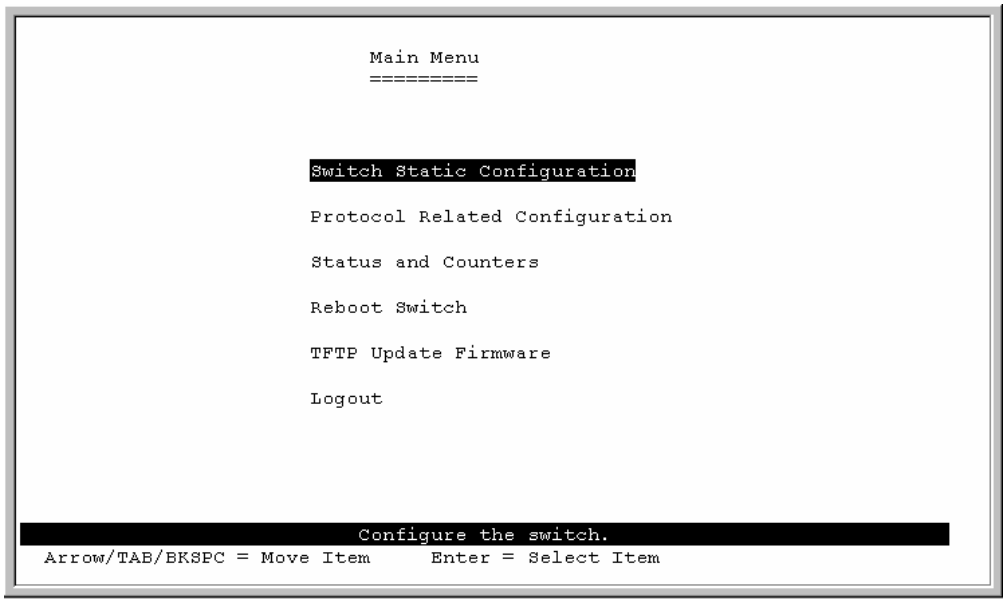
1. Set "Bits per second" at 115200 to the content window.
2. Set "Flow control" at None
3. Connects PC with the Switch, you will find login manual window on the screen then enter

4. When you are going to login a switch through the web page, you have to configure the IP address first. The default IP address /netmask / default gateway of a switch is **192.168.16.250** / 255.255.255.0 / 192.168.16.1, without making any configuration changes in advance, you can login a switch with default IP address as long as the default IP address can function properly in your network environment. Otherwise, you have to re-configure the IP address, subnet mask and default gateway. The following show how to configure the IP address of a switch.

First, login with the console port.

```
Username: admin
Password: 123
```

You will find window of "Main Menu" on the screen of the following：



5. Operation Button:

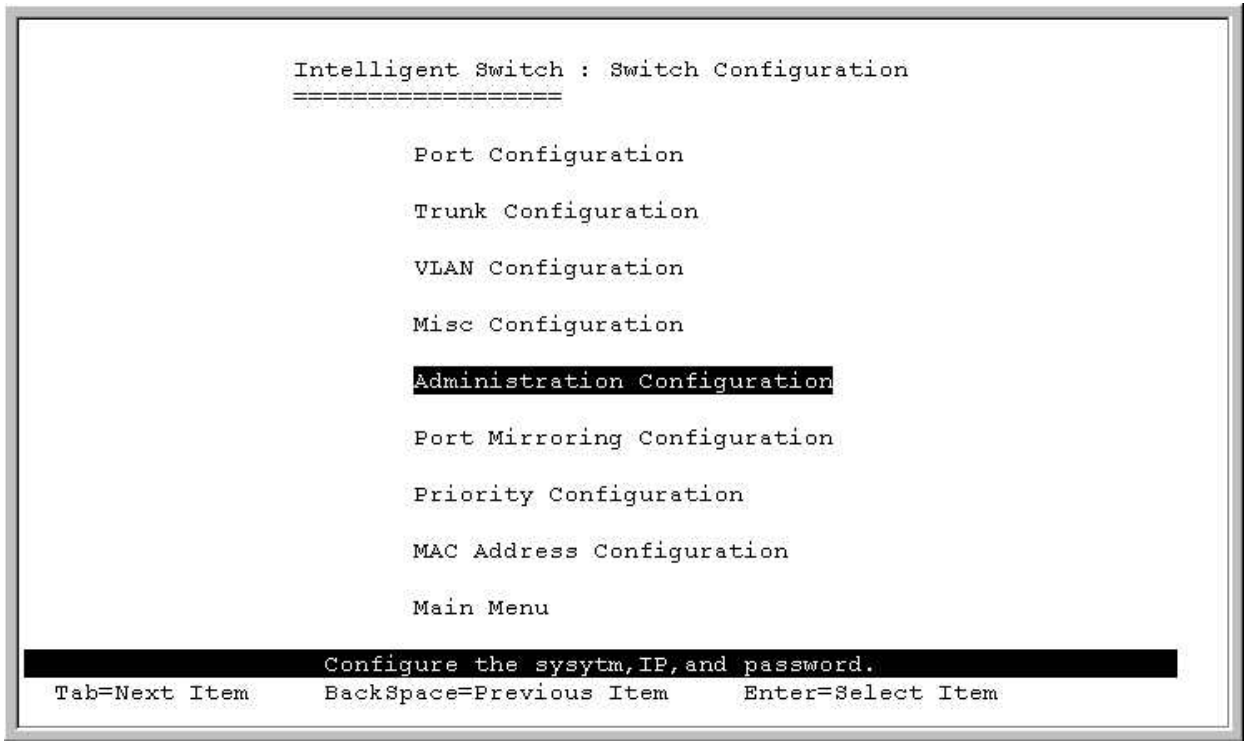
Tab=Next Item ;

BackSpace=Previous Item

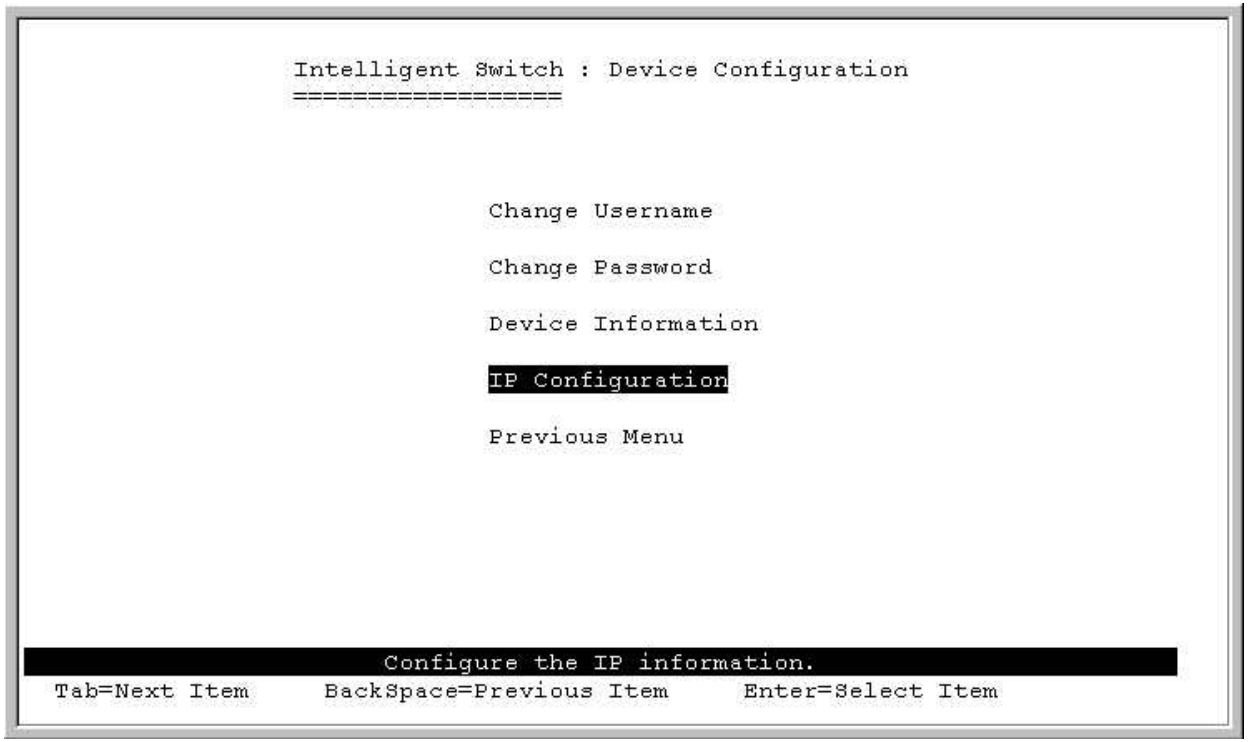
Enter=Select ItemSelect

6. Set IP Address: Please refer to the following steps

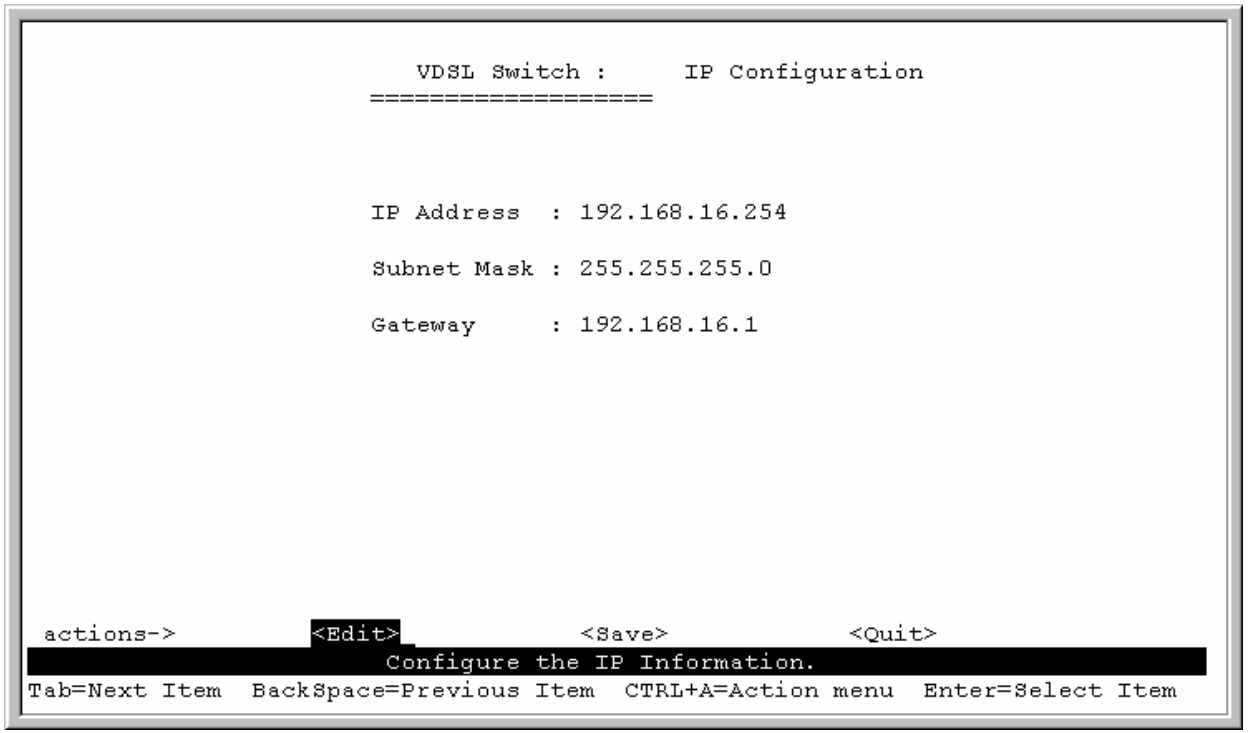
(1) Select **"Switch Static Configuration",** you can access to the Switch Configuration page.



(2) Select **"Administration Configuration",** you can access to the Device Configuration page.


Intelligent Switch : Device Configuration
Change Username
Change Password
Device Information
IP Configuration
Previous Menu
Configure the IP information.
Tab=Next Item
BackSpace=Previous Item
Enter=Select Item

(3) Select **"IP Configuration",** you can access to the IP configuration page


VDSL Switch : IP Configuration
IP Address : 192.168.16.254
Subnet Mask : 255.255.255.0
Gateway : 192.168.16.1
actions-> <Edit> <Save> <Quit>
Configure the IP Information.
Tab=Next Item BackSpace=Previous Item CTRL+A=Action menu Enter=Select Item

(4) a. Select "**Edit"** item to change IP address, Subnet Mask and Gateway
b. Use **CTRL+A** button to back actions choice
c. Select **Save** item to save change and back to System Configuration page
d. Select **Previous Menu** item to quit System Configuration page
e. Select **Main Menu** item to quit SWITCH Configuration page and back to Main Manual
f. Select **Reboot System** item
g. Select **Restart** item to reboot your SWITCH.

Now, you have changed the IP address successfully, the following chapter describes how to access the web UI. Let's go ahead.

4.1 Remote Network Management

The NS-2024E provides a built-in HTML based management interface that allows configuration of the NS-2024E via Internet Browser. Best viewed using Chrome or Firefox browsers.

In order to use the web browser to configure the device, you may need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in windows XP SP2 or above.
- Java Scripts. (Enabled by default)
- Java permissions. (Enabled by default)

4.1.1 IP Setting

You must setup the "IP Address" with the local serial console port (RS-232 Port), and then you can use this IP address to control this Ethernet Switch by **Telnet** and **WEB.** Or you can change your computer's IP domain same with Ethernet Switch. Then use the default IP address to control this Switch

1. Remote control via "Telnet"

To access the Telnet function, please execute the "run" program and enter IP address of the Ethernet Switch to connect management system. Then type User name and password.

Default User Name: **admin**
Default Password: **123**

Notes:

1. For security purpose, user can't log-in Telnet and Console port at the same time. Please logout if use completed.
2. When users use the Web user interface, you can use the Console or Telnet at the same time.

2. Network control via "WEB UI"

1.The Ethernet switch provide a WEB browser to manage and monitor, that default values are as follows：

If you need change IP address in first time，please use console mode to modify it.

Default IP Address：192.168.16.250

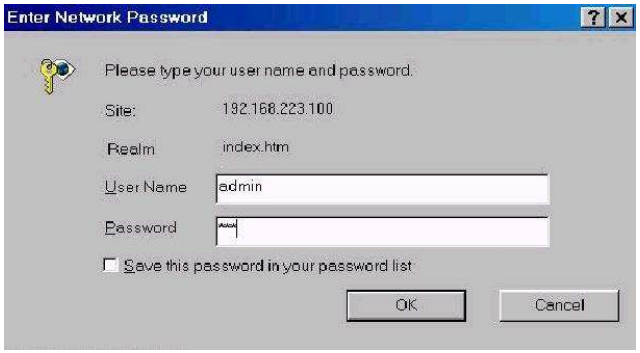
Subnet Mask： 255.255.255.0

Default Gateway：192.168.16.1

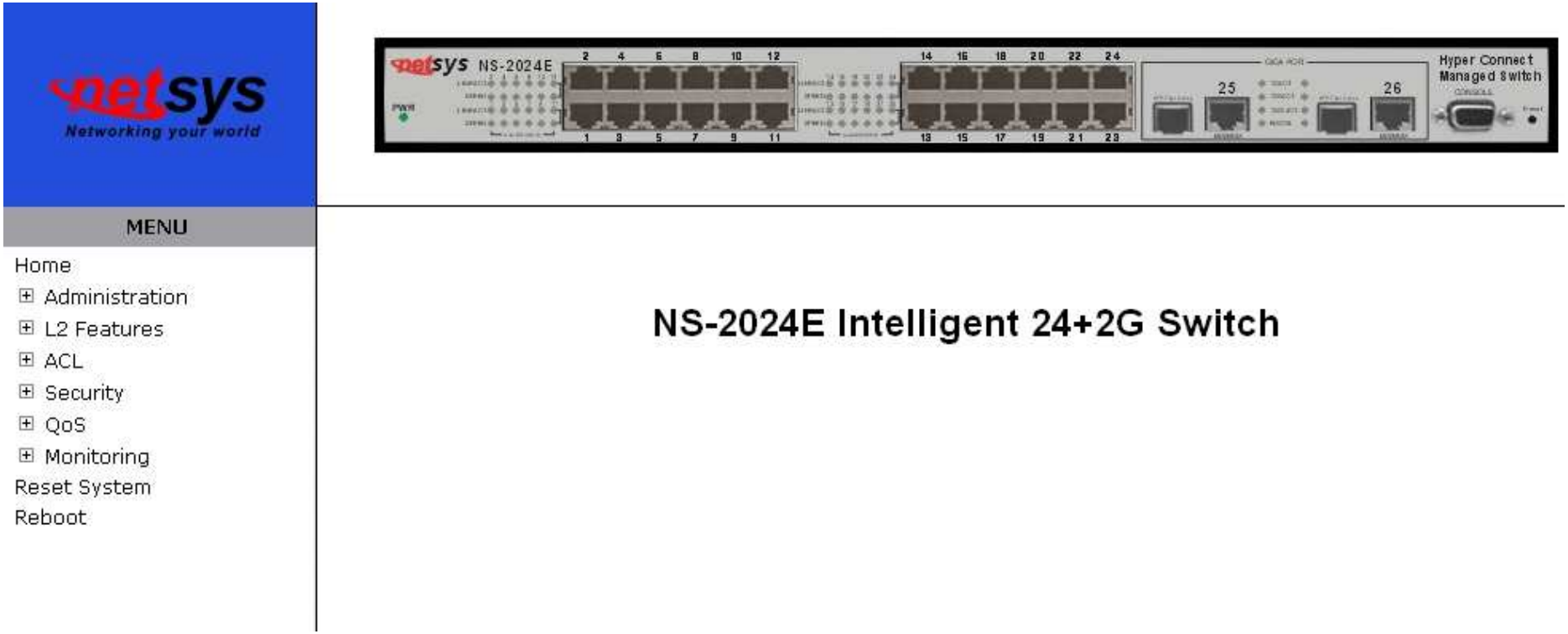
User Name：**admin**

Password： **123**

2. Please access http://192.168.16.250 via web UI to browser manage, please enter user name and password as above.



Following figure is the Web Management Home Overview:



4.2 Administration

There are many management functions can be set or performed if you expand the submenus of **Administrator** in MENU area. These functions are:

- IP address Setting
- Switch Settings
- Console Port information
- Port Controls
- SNMP Configuration
- Security Manager
- 802.1x Configuration
- Quality of Service (QoS)
- Syslog Setting
- Firmware Update
- Configuration Backup

4.2.1 IP Address Setting

User can see and modify the IP address, subnet mask and default gateway in this page, then clicks "Apply" button to confirm (save) the settings, then the switch **reboot** must be done to activate the updates. The IP address can be statically set or dynamically be assigned by enabling DHCP option.

Note:

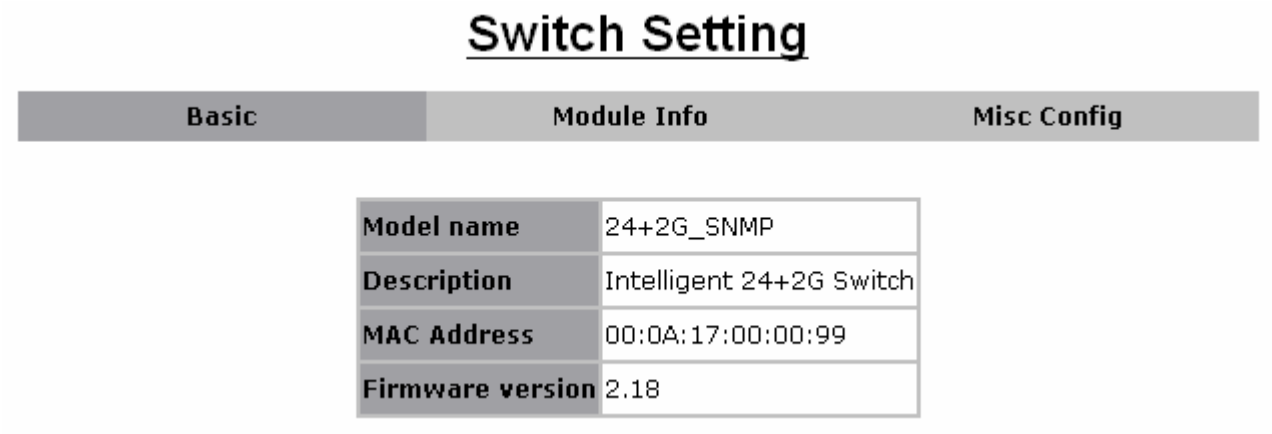
If any of the value is changed in this field, reboot is necessary.

4.2.2 Switch Setting

4.2.2.1 Basic

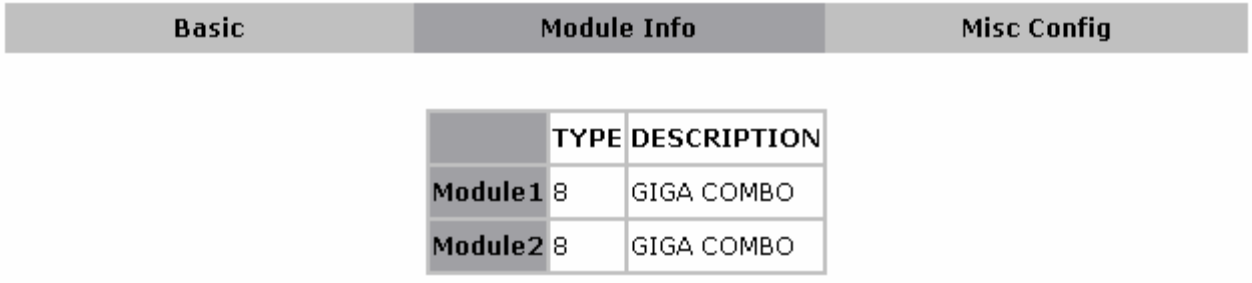
All information in **Basic** page is all read only, user can't modify the contents.

Model name: Display the switch's model name.
Description: Display the name of device type.
MAC Address: The unique hardware address assigned by manufacturer (default)
Firmware version: Display the switch's firmware version.



4.2.2.2 Module Info

All information in this field is read only, user can't modify its contents. It is only to display the module port information.



	TYPE	DESCRIPTION
Module1	8	GIGA COMBO
Module2	8	GIGA COMBO

4.2.2.3 MISC CONFIG

Basic
Module Info
Misc Config
MAC Table Address Entry
Age-Out Time: 300 seconds (6~1572858,must multiple of 6,default is 300s)
Turn On Port Interval: 0 seconds (0~3600 seconds, interval time between turning off and turning on port for flooding CPU port, 0:disable)
Broadcast Storm Filter Mode: OFF
Broadcast Storm Filter Packet select
Broadcast Packets
IP Multicast
Control Packets
Flooded Unicast/Multicast Packets
Collisions Retry Forever : Disable
Hash Algorithm : CRC-Hash
IP/MAC Binding : Disable
802.1x Protocol : Disable
Apply
Default
Help

MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 6~1572858 seconds. Default is 300 seconds. The value is a multiple of 6.

Turn on Port Interval: while flooding CPU port at the speed of 4MB/s or larger, system will close relative port.
And system will open this port using this interval value.0 represents system will never enable this after close it for flooding CPU.

Broadcast Storm Filter Mode: To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's ingress bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold value are 1/2, 1/4, 1/8, 1/12, and off.

Broadcast Storm Filter Packets Select: To select broadcast storm Filter Packets type. If no packets type by selected, mean can not filter any packets .The Broadcast Storm Filter Mode will show OFF. Collisions Retry Forever: In half duplex, collision-retry maximum is 16, 32, or 48 times and packet will be dropped if collisions still happen. In default (Disable), system will retry forever if collisions happen.

Hash Algorithm: Select Hash Algorithm.
IP/MAC Bing: Enable or disable SMAC and SIP binding.
802.1x Protocol: Enable or disable 802.1x protocol.

4.2.3 Console Port Information

Console is a standard UART (RS-232) interface to communicate with Serial Port.

User can use windows HyperTerminal program to link the switch. Connect To -> Configure:

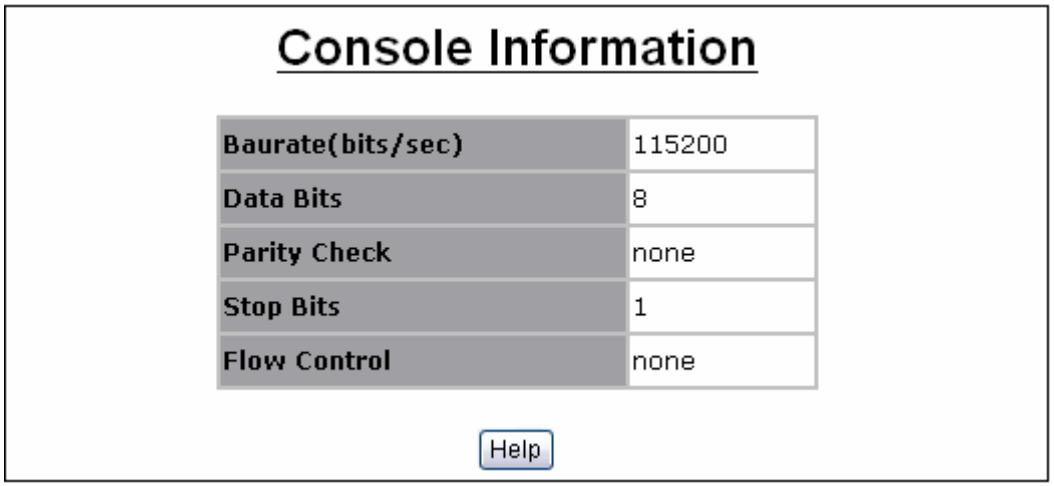
Bits per seconds: **115200**

Data bits: **8**

Parity: **none**

Stop Bits: **1**

Flow control: **none**



4.2.4 Port Configuration

4.2.4.1 Port Controls

The following webpage is to provide the display and modification for the port settings. Use the dropdown in Port field to select one or multiple ports in the upper control area. The lower display area will show the port settings for the selected port(s). Use the other control fields in the upper area to modify the port settings for the selected port(s). Press Apply to save and activate the port settings.

Port Controls

Port	State	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)		Security	BSF	Jumbo Frame
						Ingress	Egress			
Port1 Port2 Port3 Port4	Enable	Auto	1000	Full	Enable	0	0	☐	Enable	Enable

Apply

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			

State: User can disable or enable this port.

Negotiation: User can set auto negotiation mode is Auto, Nway (specify the speed/duplex on this port and enable auto-negotiation), Force of per port.

Speed: User can set 100Mbps or 10Mbps speed on Port1~Port24. User can set 1000Mbps, 100Mbps or 10Mbps speed on Port25~Port26 (depend on module card mode).

Duplex: User can set full-duplex or half-duplex mode of per port.

Flows control:
Full: User can set flow control function is enable or disable in full mode.
Half: User can set backpressure is enable or disable in half mode.

Rate Control: port1 ~ port 24, supports by-port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. Device will perform flow control or backpressure to confine the ingress rate to meet the specified rate.

Ingress: Type the port effective ingress rate. The valid range is 0 ~ 8000. The unit is 128Kbps.
0: disable rate control.
1 ~ 8000: valid rate value

Egress: Type the port effective egress rate. The valid range is 0 ~ 8000. The unit is 128Kbps.
0: disable rate control.

1 ~8000: valid rate value.

Port Security: A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, and then click Apply to change on this page.

BSF: User can disable/Enable port broadcast storm filtering option by port. The filter mode and filter packets type can be select in Switch Setting > Misc Config page.

Jumbo Frame: User can disable/Enable port jumbo frame option by port. When port jumbo frame is enable, the port forward jumbo frame packet

4.2.4.2 Port Sniffer

The Port Sniffer (mirroring) is a method for monitor traffic in switched networks. Traffic through a port can be monitored by one specific port. That is, traffic goes in or out a monitored port will be duplicated into sniffer port.

Sniffer Type: Select a sniffer mode: Disable / Rx / Tx / Both.
Analysis (Monitoring) Port: It' means Analysis port can be used to see the traffic on another port you want to monitor. You can connect Analysis port to LAN analyzer.
Monitored Port: The monitor port traffic will be copied to Analysis port. You can select one monitor ports in the switch. User can choose which port that they want to monitor in only one sniffer type.

Note:

1. The Analysis port is dedicated for monitoring usage. That is the ordinary port function will be unavailable.
2. If you would like to disable this function, you need select monitor port to none.

Port Sniffer

Sniffer Type: RX

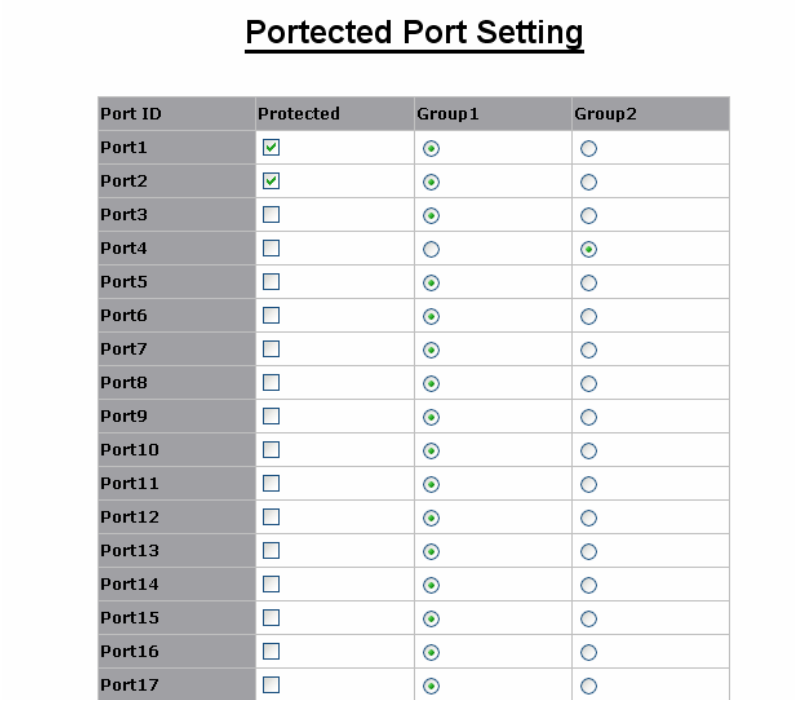
Analysis Port: Port1

Port	Monitor
Port1	○
Port2	○
Port3	○
Port4	○
Port5	○
Port6	○
Port7	○
Port8	○
Port9	○
Port10	○
Port11	○
Port12	○
Port13	○
Port14	○
Port15	○

4.2.4.3 Protected Port

There are two protected port groups. Ports in different groups can't communicate each other.

In the same group, protected ports can't communicate each other, but can communicate with unprotected ports. Unprotected ports can communicate with any ports, including protected ports. In default, all ports are in Group1 and not protected.



For example, in the above configuration page for protected port, Port4 in Group2, other ports in Group1, and both Port1& Port2 are protected. These settings provide Port4 can't communicate with other ports in Group1. Port1 & Port2 can't communicate each other but can communicate with other ports in Group1.

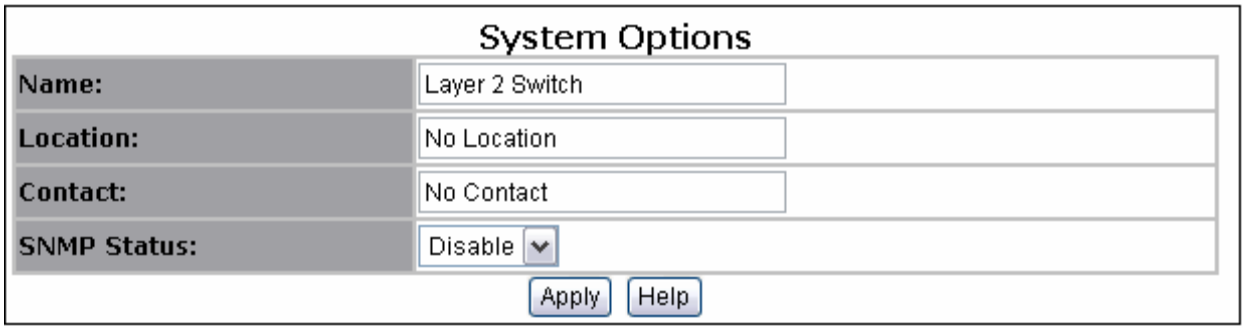
4.2.5 SNMP Configuration

Any Network Management platform running the simple Network Management Protocol (SNMP) can manage the switch, provided the Management Information Base (MIB) is installed correctly on the management station. The SNMP is a Protocol that governs the transfer of information between management station and agent.

4.2.5.1 System Options

Use this page to define management stations as trap managers and to enter SNMP community strings. User can also define a name, location, and contact person for the switch. Fill in the system options data, and then click Apply to update the changes on this page.

Name: Enter a name to be used for the switch.
Location: Enter the location of the switch.
Contact: Enter the name of a person or organization.
SNMP Status: Enable/Disable SNMP Function



4.2.5.2 Community strings

Serve as passwords and can be entered as one of the following:

RO: Read only. Enables requests accompanied by this string to display MIB-object information.

RW: Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

4.2.5.3 Trap Manager

Trap Manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.

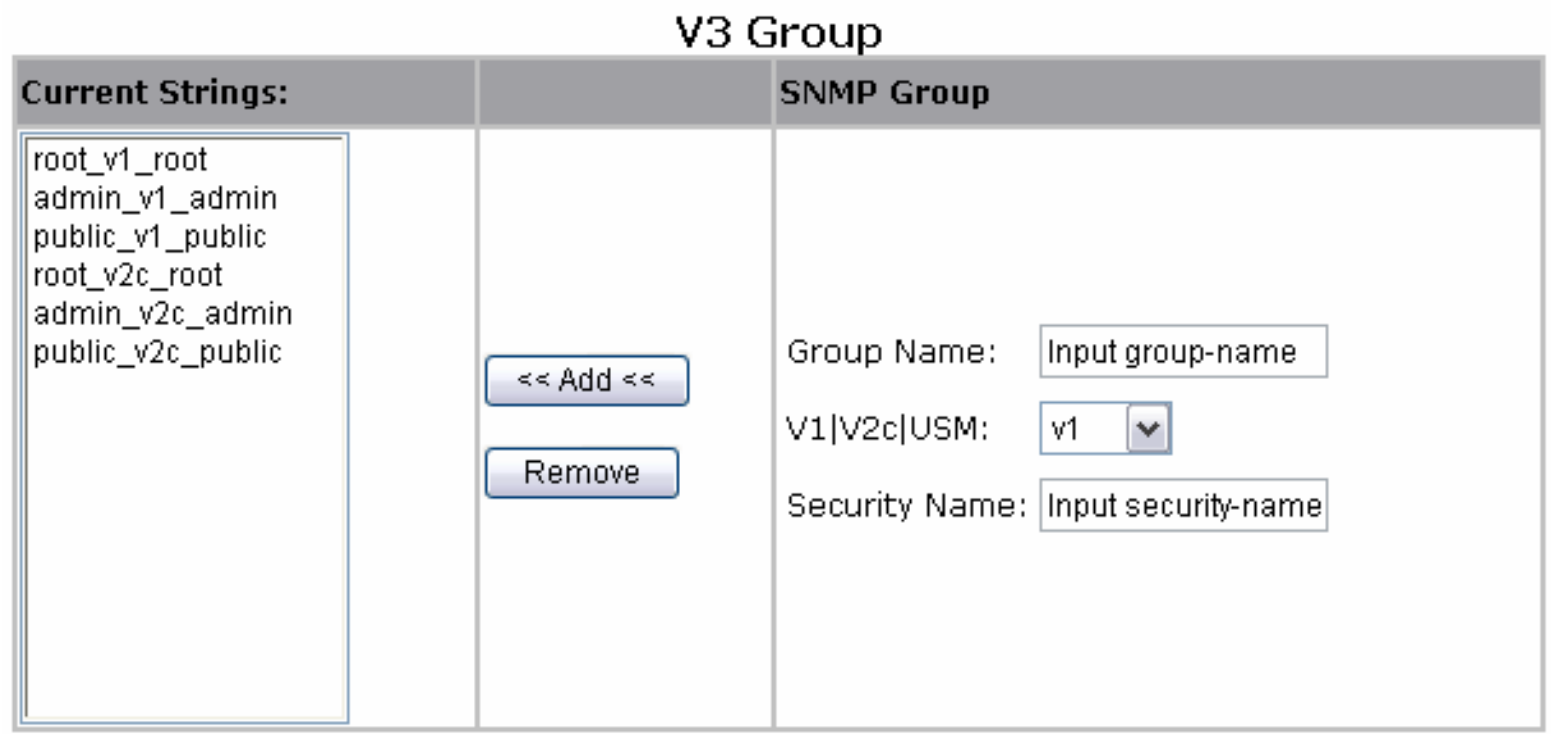
4.2.5.4 SNMPv3 Group

Maintain SNMPv3 group.

Group Name: specifies the group name.

v1 | v2c | USM: specifies the security model.

Security Name: specifies the security name.



4.2.5.5 SNMPv3 View

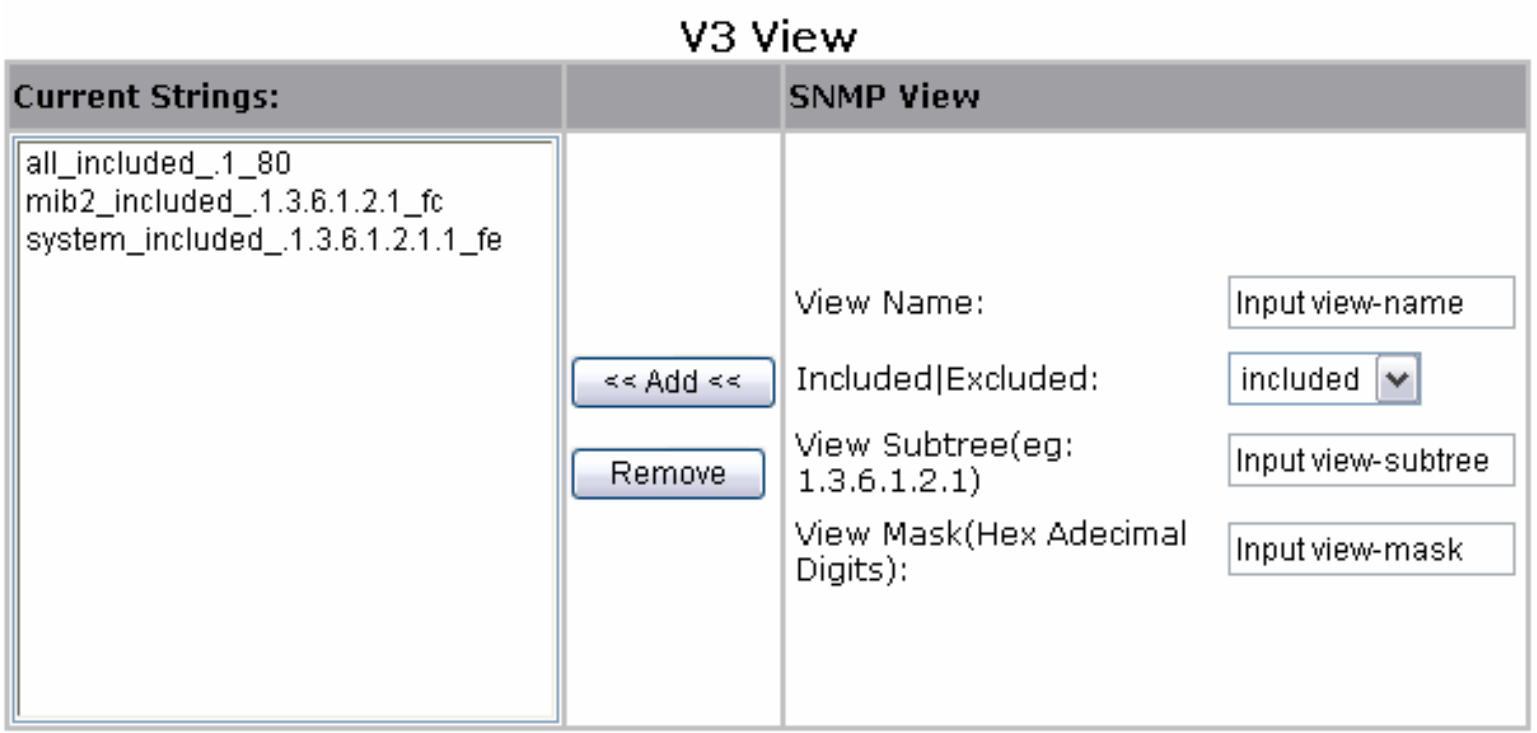
Maintain SNMPv3 view.

View Name: specifies the view name.

Included | Excluded: specifies the view type.

View Subtree: specifies the view subtree (e.g. .1.3.6.1.2.1).

View Mask: specifies the view mask, in hexadecimal digits.



4.2.5.6 SNMPV3 ACCESS

Group Name: specifies the group name.

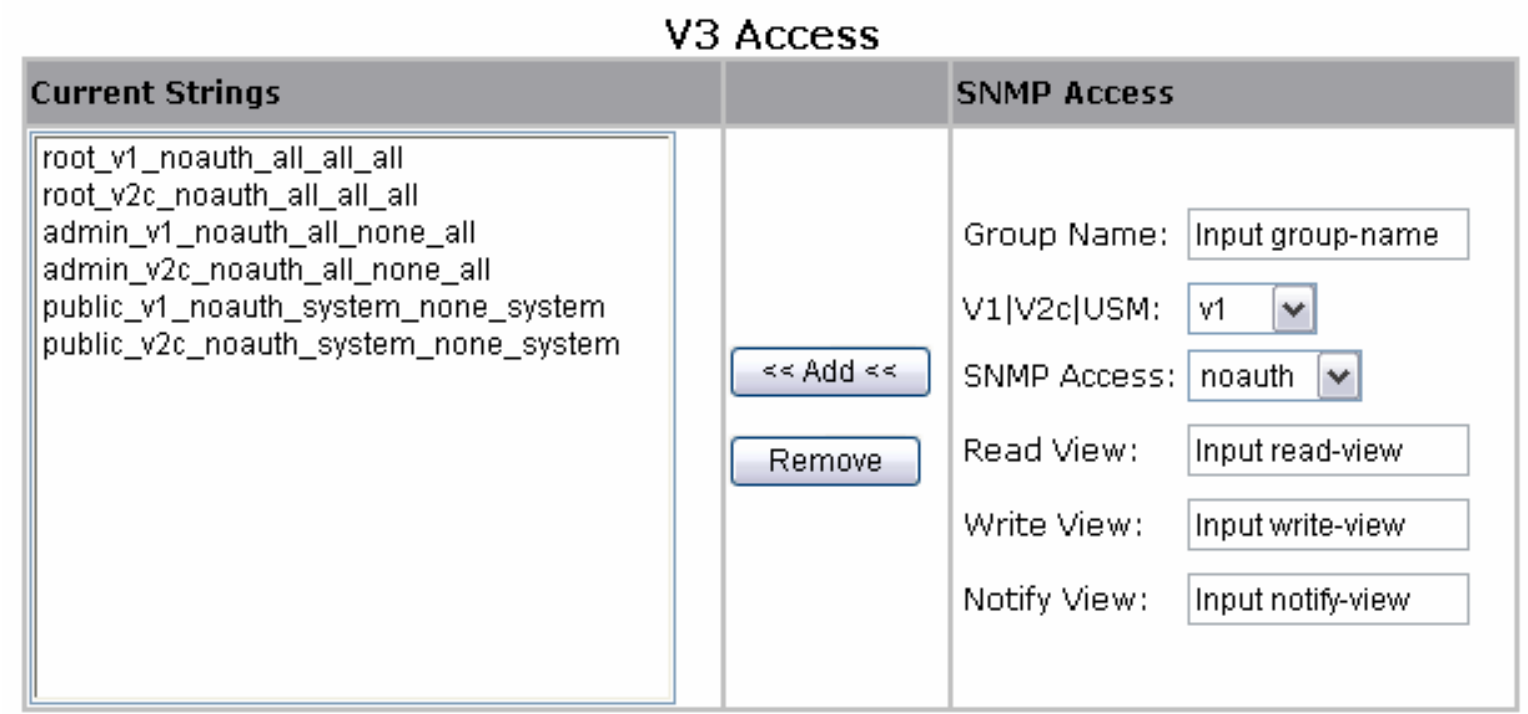
v1 | v2c | USM: specifies the security model.

SNMP Access: specifies the security level (**noauth | auth | authpriv**)

Read View: specifies the access read view name.

Write Name: specifies the access write view name.

Notify Name: specifies the access notify view name.



4.2.5.7 SNMPv3 USM-User

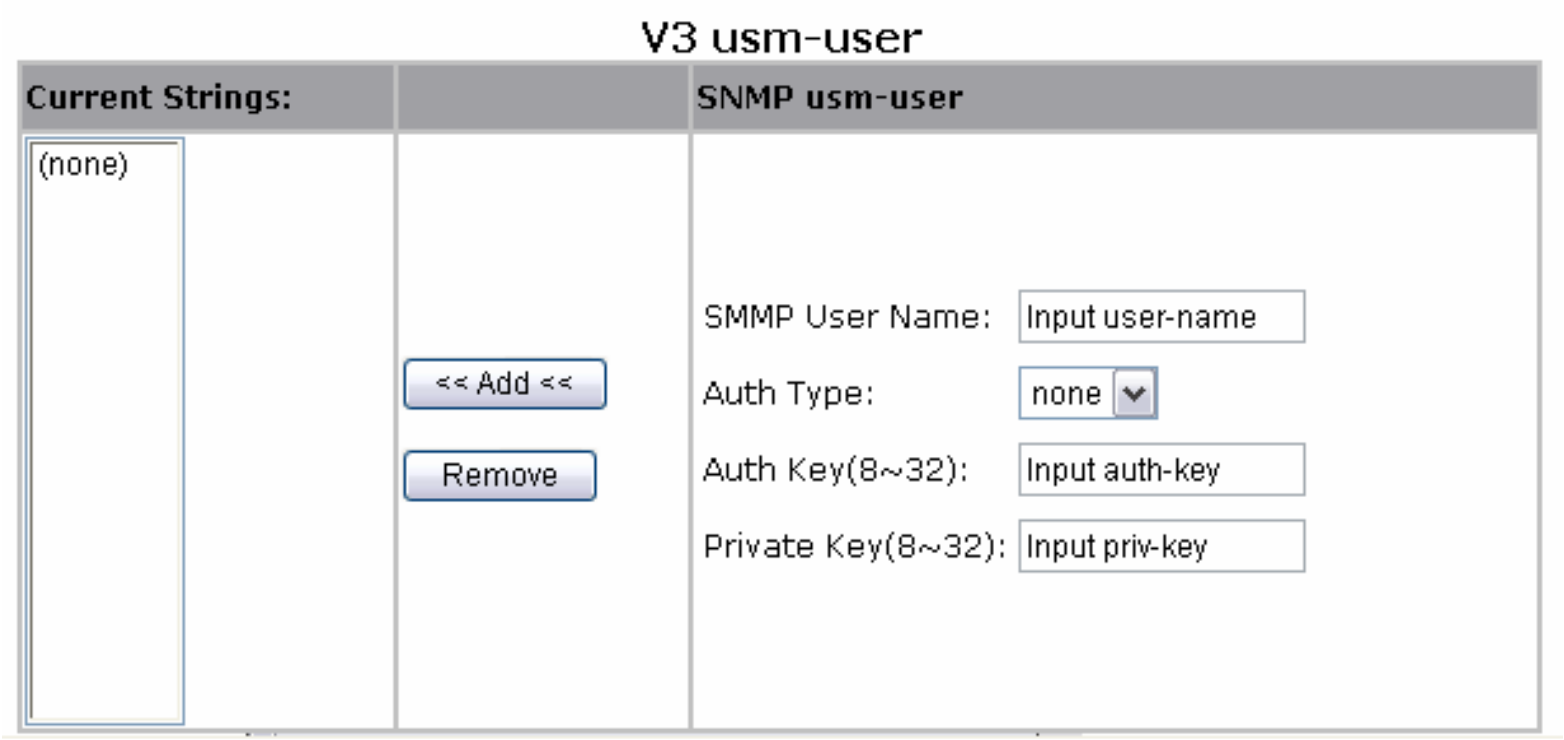
Maintain SNMPv3 USM-user.

User Name: Specifies the user name (should be the security name defined in group)

Auth Type: Specifies the authentication type (**md5 / none**)

Auth-Key: Specifies the authentication key (8~32 chars)

Private Key: Specifies the encrypt key (8~32 chars)

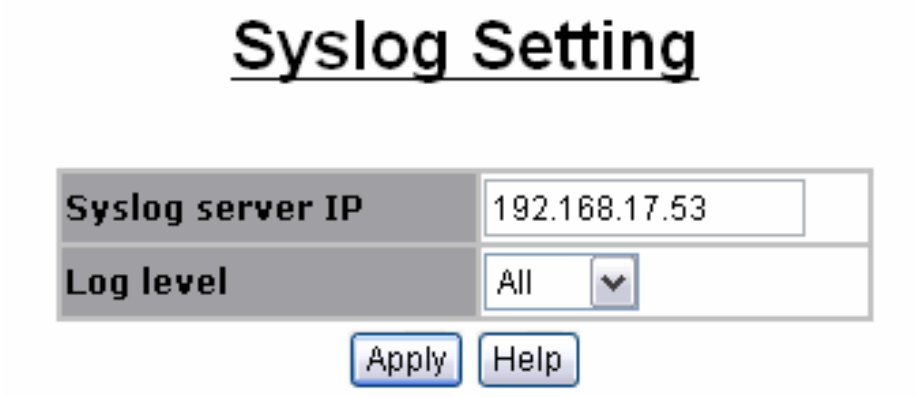


4.2.6 Syslog

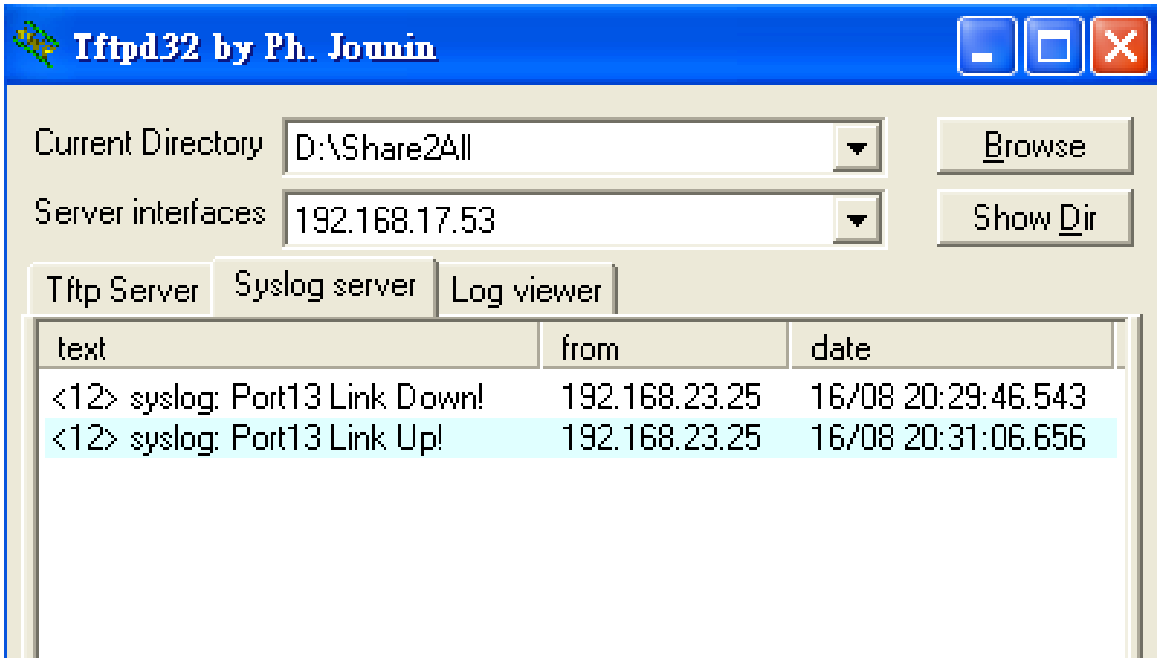
This system supports syslog sent to a remote syslog server. Currently system will do syslog for 3 events: **cold start, warm start and link change**. In this page, user needs to setup the following parameters to activate the syslog:

Syslog server IP: The IP address of remote syslog server
Log level: None / Major / All

Then click Apply button to activate the syslog function.



The following example figure shows the syslog server application (e.g. Tftpd32.exe) got the messages from switch which link status is changed on port13.

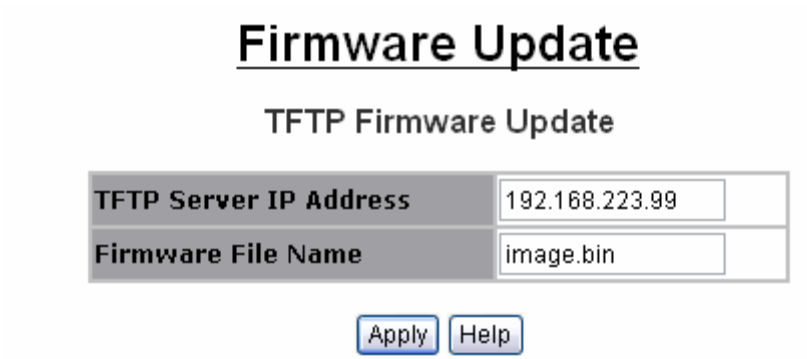


4.2.7 Firmware Update

This system supports firmware update through two different ways: TFTP and HTTP.

4.2.7.1 TFTP Update

Use this page to assign a TFTP server IP address and an existing firmware image file. Then press Apply button to start the firmware update process.

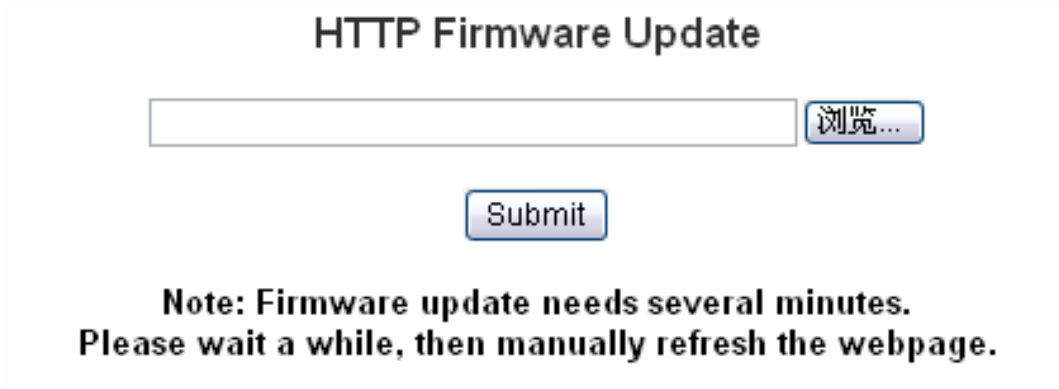


The firmware image will first update to the RAM area in system. Hit the Update Firmware button to confirm to write to the system's flash memory.

When the whole process is completed, system needs to be rebooted by pressing the reboot button to activate the new firmware.

4.2.7.2 HTTP Update

An alternative for firmware updating is using HTTP transfer. Just like the file copy in Windows, select the valid firmware image file to be uploaded to the switch and hit Submit to start the updating process. This is easier than ordinary TFTP file transfer.


HTTP Firmware Update
浏览...
Submit
Note: Firmware update needs several minutes.
Please wait a while, then manually refresh the webpage.

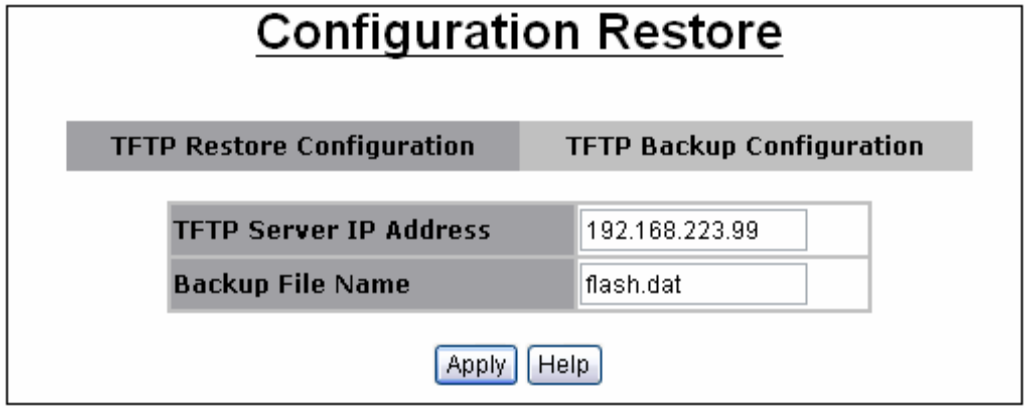
When complete firmware image upload, the system will automatically restart.

4.2.8 Configuration Backup

Just like the firmware update, this system also supports configuration backup/restore through either TFTP or HTTP transfer.

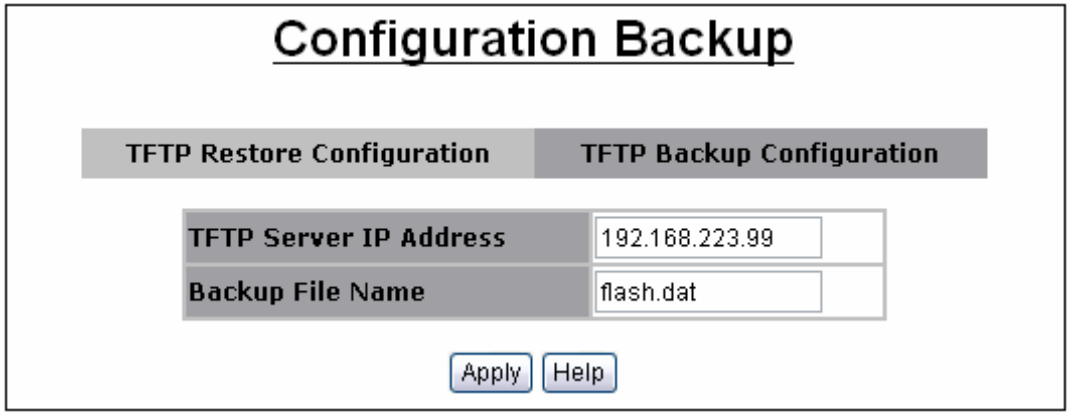
4.2.8.1 TFTP Restore Configuration

Use this page to assign a TFTP server IP address and an existing configuration filename to be restored. Then press Apply button to start the restore process.



4.2.8.2 TFTP Backup Configuration

Use this page to assign a TFTP server IP address and a filename to be stored. Then press Apply button to start the backup process.


Configuration Backup
TFTP Restore Configuration
TFTP Backup Configuration
TFTP Server IP Address
192.168.223.99
Backup File Name
flash.dat
Apply
Help

4.3 L2 Features

This switch provides the following L2 features:

- VLAN Configuration
- Trunking (Port Aggregation)
- Forwarding & Filtering
- Spanning Tree (STP)
- DHCP Relay & Option 82
- LLDP **(optional)**

4.3.1 VLAN Configuration

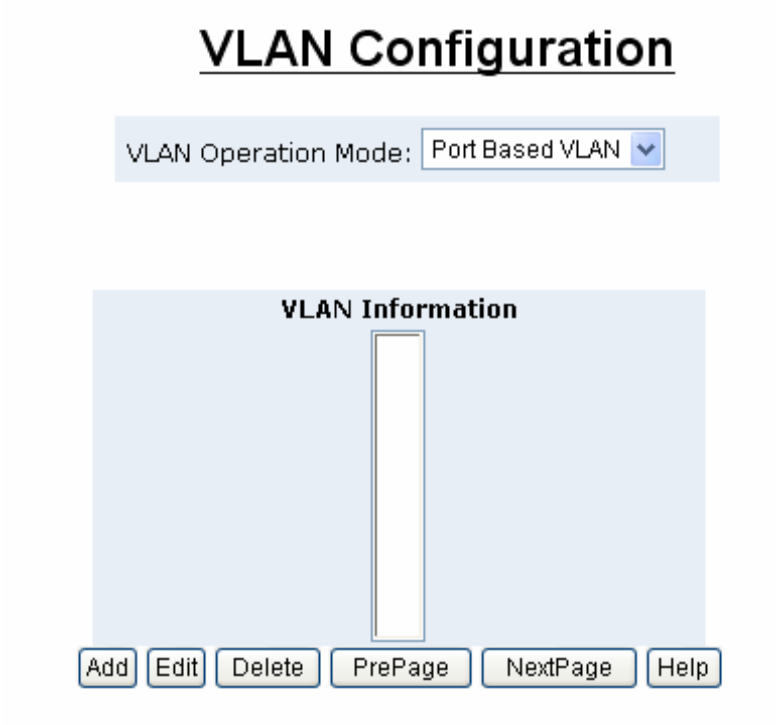
A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

This switch supports port-based, 802.1Q (tagged-based) or no VLAN in web management page. In default, 802.1Q VLAN is enabled for common and advanced operations.

- Static VLAN
- GVRP VLAN
- QinQ VLAN

4.3.1.1 Static VLAN

4.3.1.1.1 Port Based VLAN



First select Port-based VLAN in VLAN Operation Mode. Then click Add to create a new VLAN group.

Enter the VLAN name, group ID and select the members for the new VLAN. Then click Apply to activate the setting.

If there are many groups that over the limit of one page, you can click the Next Page to view other VLAN groups.

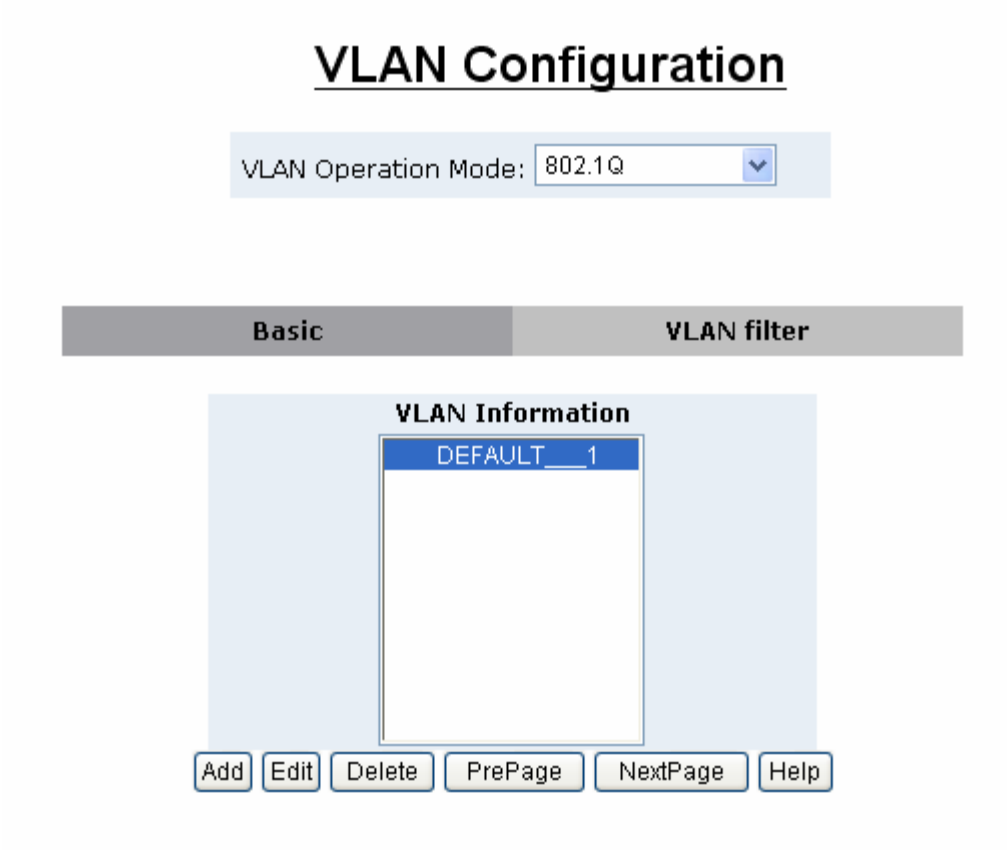
Note:

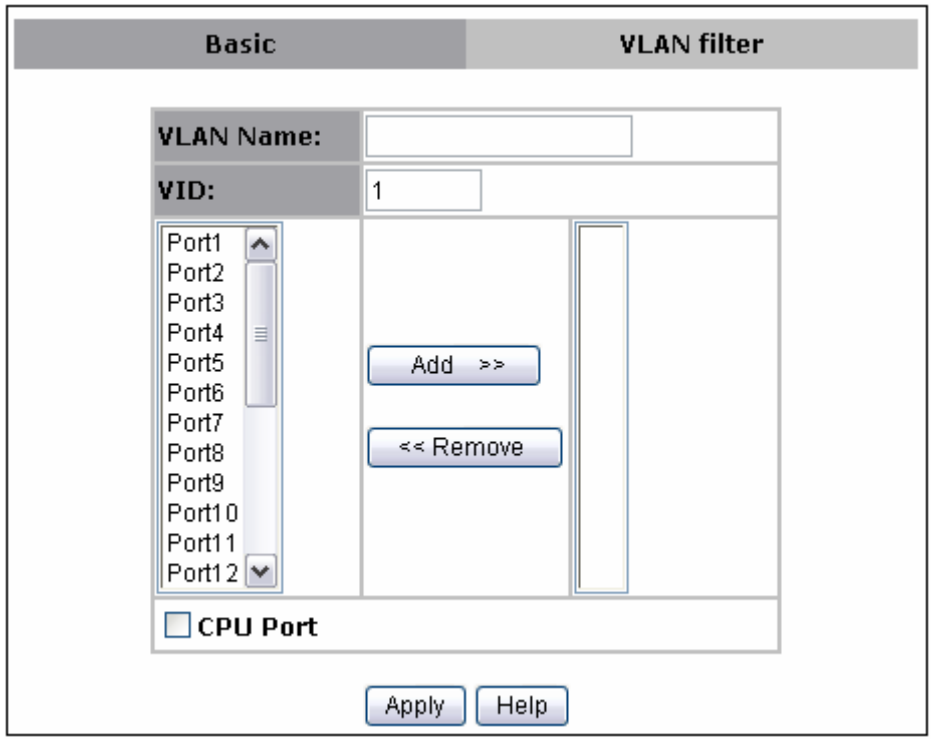
If VLAN trunk groups has exist, you can see it (ex: TRK1, TRK2…) in the select menu of ports. Click "edit" button and then you can edit the member of the VLAN group.

4.3.1.1.2 802.1Q VLAN

In this page, user can create 802.1Q (tag-based) VLAN.

There are up to 512 VLAN groups to provide configuration. While VLAN Operation Mode is changed to 802.1Q VLAN, all ports on the switch belong to default VLAN group which VID is 1. The default VLAN group can't be deleted.





Basic

Create a VLAN and add tagged member ports to it.

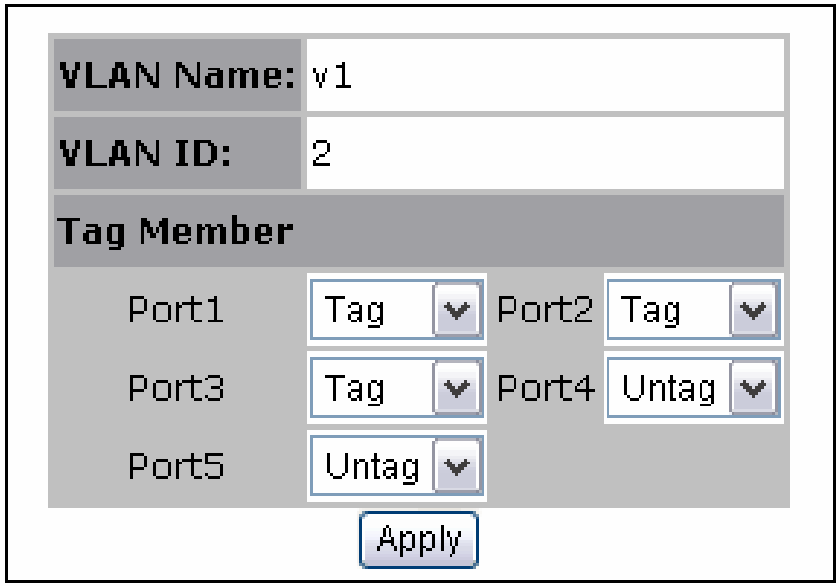
1. From the main menu, click Administrator VLAN configuration, click Add then you will see the page as follow.

2. Type a name for the new VLAN.

3. Type a VID (1~4094). The default is 1.

4. From the Available ports box, select ports to add to the switch and click "Add >>". If the trunk groups exist, you can see it in here (ex: TRK1, TRK2…), and you can configure it is the member of the VLAN or not.

5. Click Next. Then you can view the page as follow：

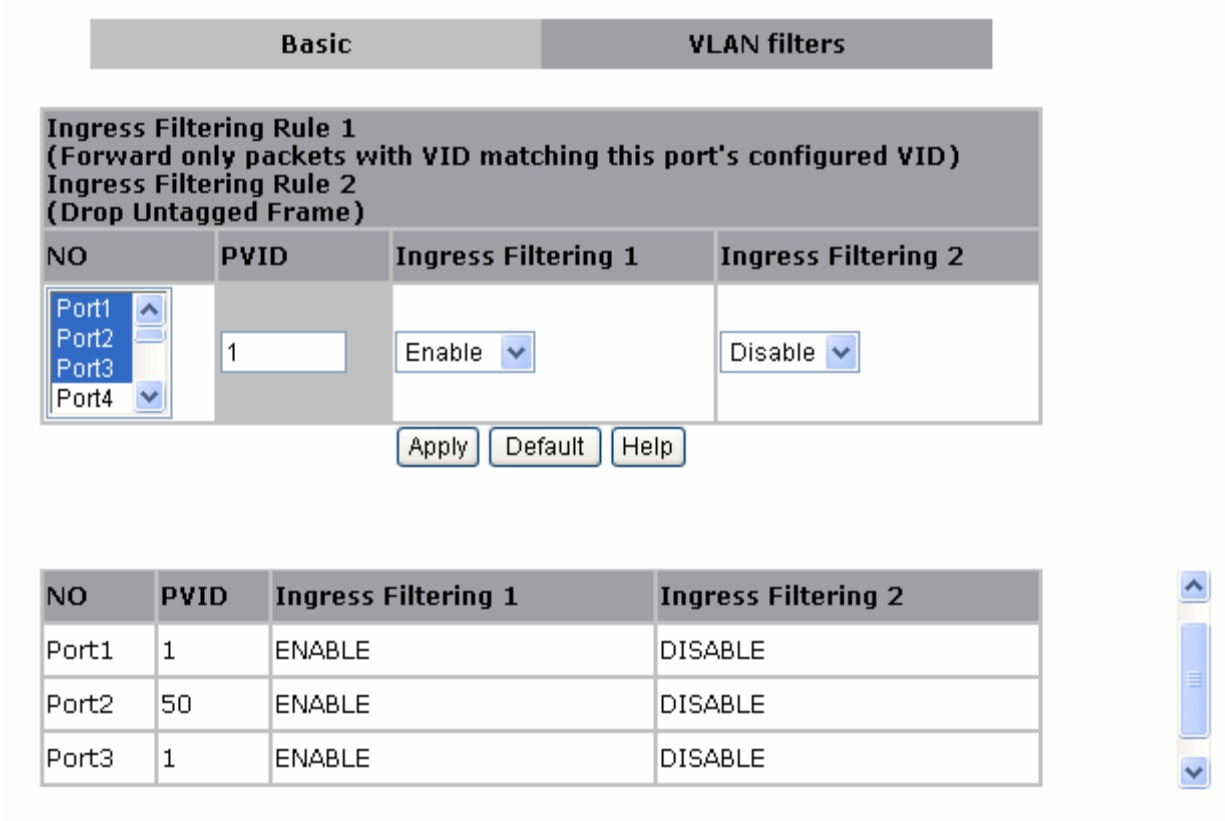


6. Uses this page to set the outgoing frames are VLAN-Tagged frames or no. Then click Apply.

Tag: outgoing frames with VLAN-Tagged.

Untag: outgoing frames without VLAN-Tagged.

VLAN Filters



Port NO.

Port number(s) to be assigned to see or configure the settings.

Port VID (PVID)

Port VLAN ID will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you

want to participate in the VLAN but that don't support tagging. This switch allows user to set one PVID for each port, the range is 1~4094, default PVID is 1. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. This switch has two ingress filtering rule as follows:

Ingress Filtering Rule 1: A forward only packet with VID matching this port's configured VID.

Ingress Filtering Rule 2: Drop Untagged Frame.

4.3.1.2 GVRP VLAN

4.3.1.2.1 GVRP Setting

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch, the switch will automatically add that device to the existing VLAN

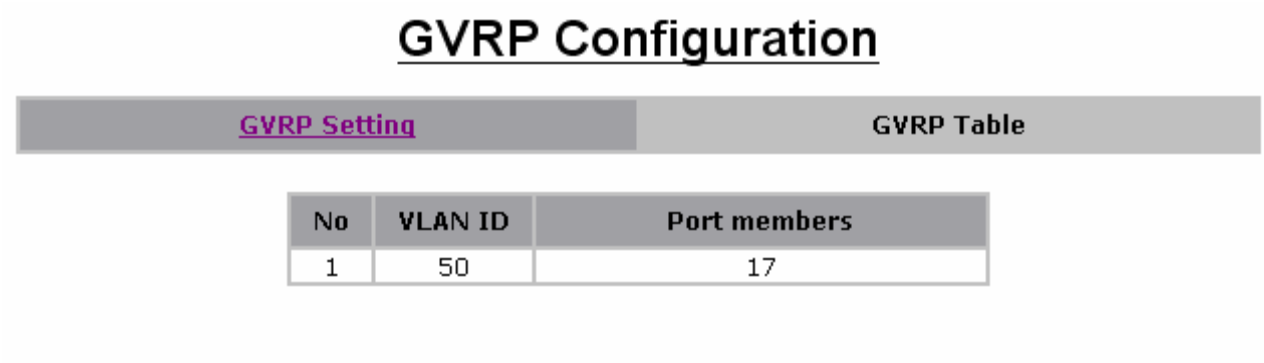
GVRP can be enabled per port basis. To enable GVRP function for a port, both global GVRP and special port GVRP are required to configure.

GVRP Configuration

GVRP Setting | GVRP Table

GVRP	Enable
Port	GVRP
Port1	☐
Port2	☐
Port3	☐
Port4	☐
Port5	☐
Port6	☐
Port7	☐
Port8	☐
Port9	☐
Port10	☐
Port11	☐
Port12	☐
Port13	☐
Port14	☐
Port15	☐
Port16	☐
Port17	☑

4.3.1.2.2 GVRP Table



In this page, the VLAN group(s) dynamically created by GVRP can be displayed with VID and port member(s).

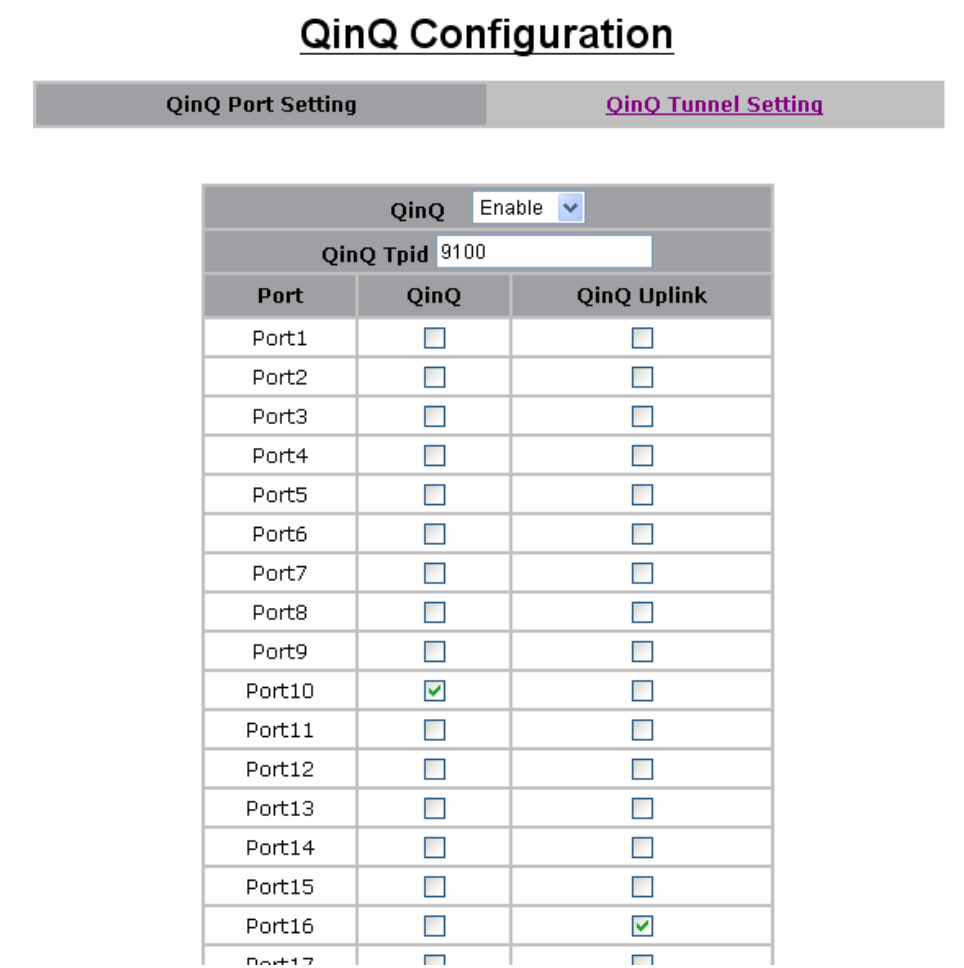
4.3.1.3 QinQ VLAN

4.3.1.3.1QinQ Port Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification. Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support QinQ is called a QinQ user-port. A port configured to support QinQ Uplink is called a QinQ uplink-port.

To enable QinQ function, the global **QinQ** option, QinQ **Tpid** and specified port-based QinQ **User** or **Uplink** port option need to

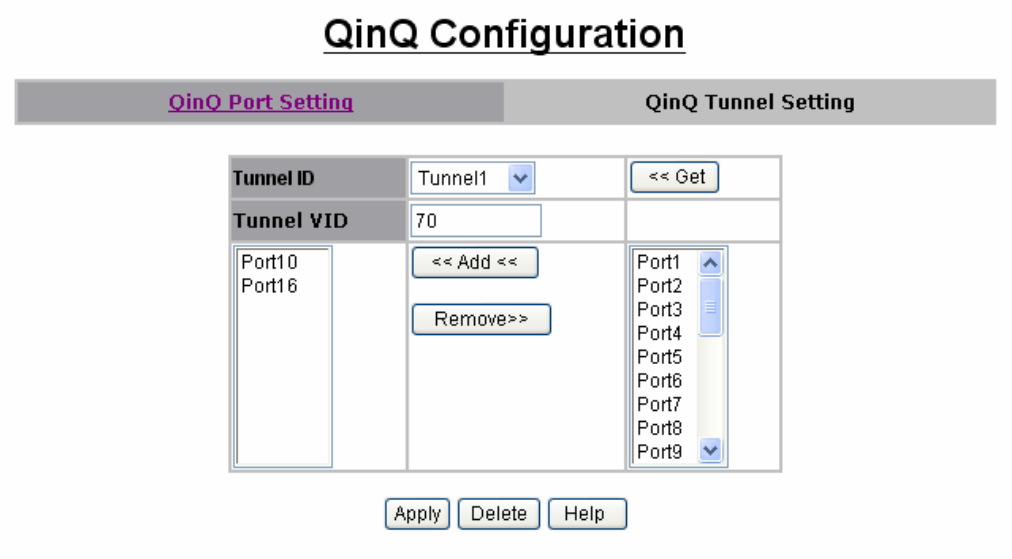
be configured.



4.3.1.3.2 QinQ Tunnel Setting

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. QinQ tunnel is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. When you configure QinQ tunnel, you assign the QinQ user-port and uplink-port to a VLAN ID that is dedicated to QinQ tunnel.

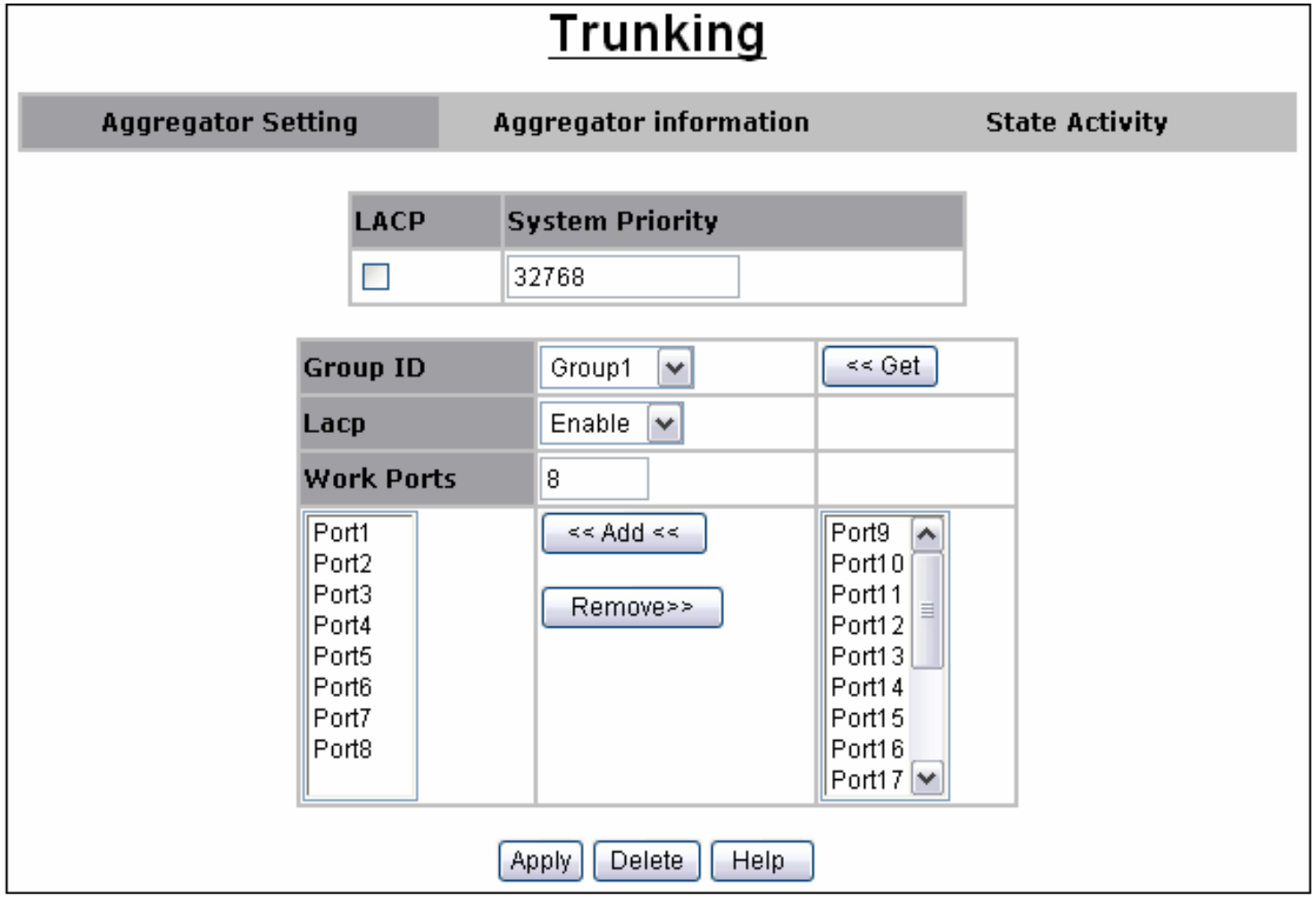
To add QinQ tunnel, you first select QinQ Tunnel ID, then fill VLAN ID QinQ dedicated to QinQ tunnel, and select user-port and uplink-port to be added to QinQ tunnel.



4.3.2 Trunking

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. In conclusion, Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, more detail information refers to IEEE 802.3ad.

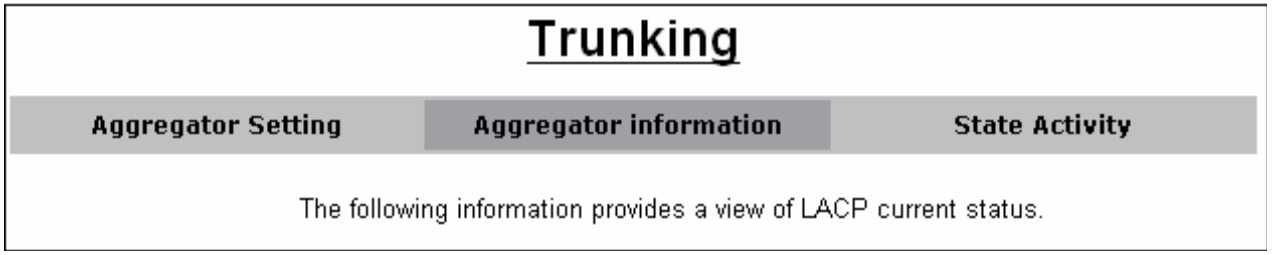
4.3.2.1 Aggregator Setting



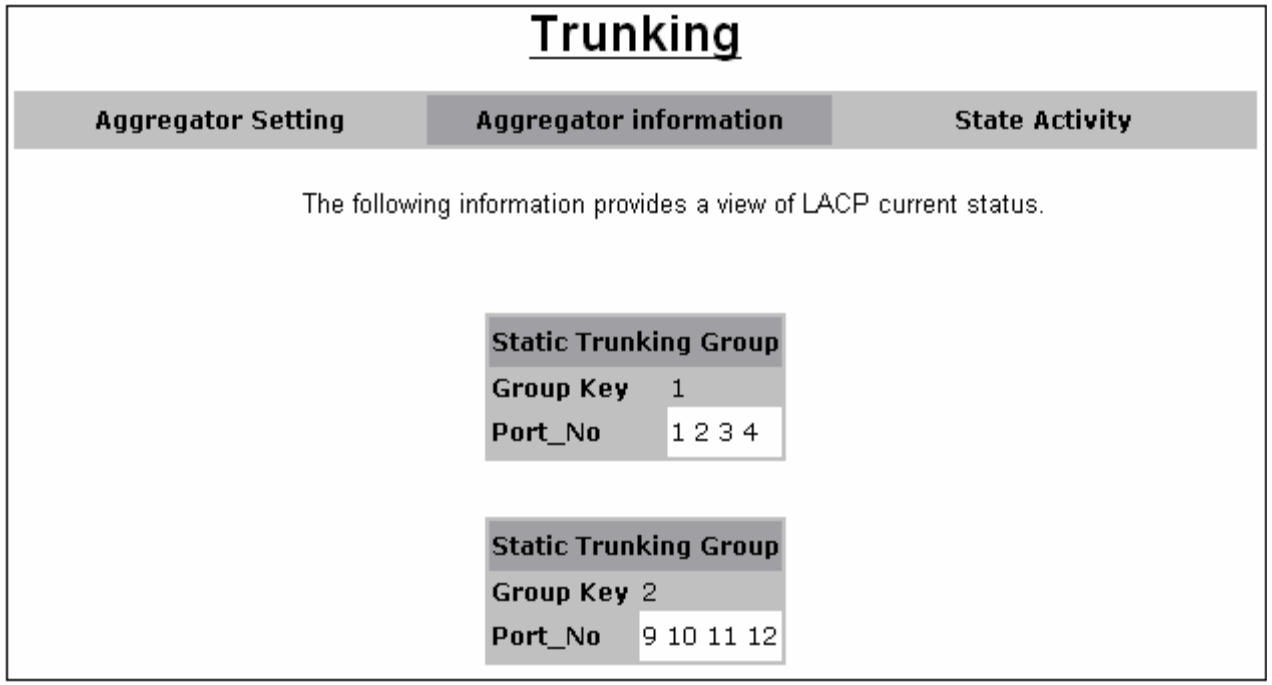
System Priority: A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
Group ID: Up to seven trunk groups can be configured. Choose the "Group ID" and click << Get to retrieve the trunk group.
LACP: If enabled, the group is LACP static trunk group. If disabled, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
Work ports: Allow max eight ports can be aggregated at the same time. If LACP static trunk group, the exceed ports is standby and able to aggregate if work ports fail. If local static trunk group, the number must be as same as the group member ports. Select the ports to join the trunk group. Allow max 8 ports can be aggregated at the same time. If LACP enabled, you can configure LACP Active/Passive status in each port on State Activity page.

4.3.2.2 Aggregator Information

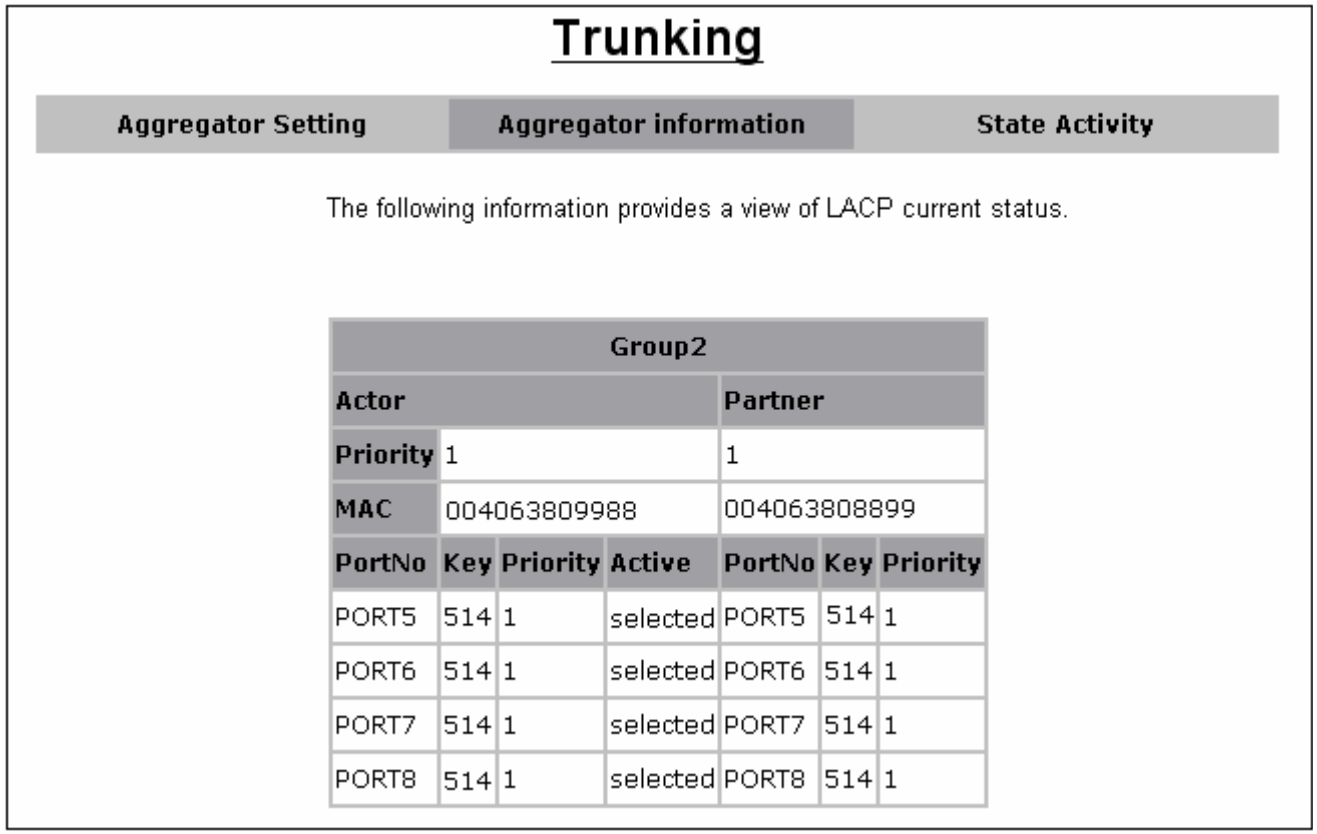
When you are setting LACP aggregator, you can see relation information in here. The following page shows no group active and no LACP related data.



This page shows some static trunk groups are created.



This page shows actor and partner trunks one group.



Trunking

Aggregator Setting | Aggregator information | State Activity

The following information provides a view of LACP current status.

Group2						
Actor				Partner		
Priority	1			1		
MAC	004063809988			004063808899		
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT5	514	1	selected	PORT5	514	1
PORT6	514	1	selected	PORT6	514	1
PORT7	514	1	selected	PORT7	514	1
PORT8	514	1	selected	PORT8	514	1

4.3.2.3 State Activity

Active (select): The port automatically sends LACP protocol packets.

N/A (no select): The port does not automatically sends LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

1. A link that has either two active LACP ports or one active port can perform dynamic LACP trunking.

A link has two N/A LACP ports will not perform dynamic LACP trunking because both ports are waiting for and LACP protocol packet from the opposite device.

2. If you are active LACP's actor, when you are select trunking port, the active status will be created automatically.

Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	☑ Active
3	☑ Active	4	☑ Active
5	N/A	6	N/A
7	N/A	8	N/A
9	☑ Active	10	☑ Active
11	☑ Active	12	☑ Active
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A
25	N/A	26	N/A

Apply Help

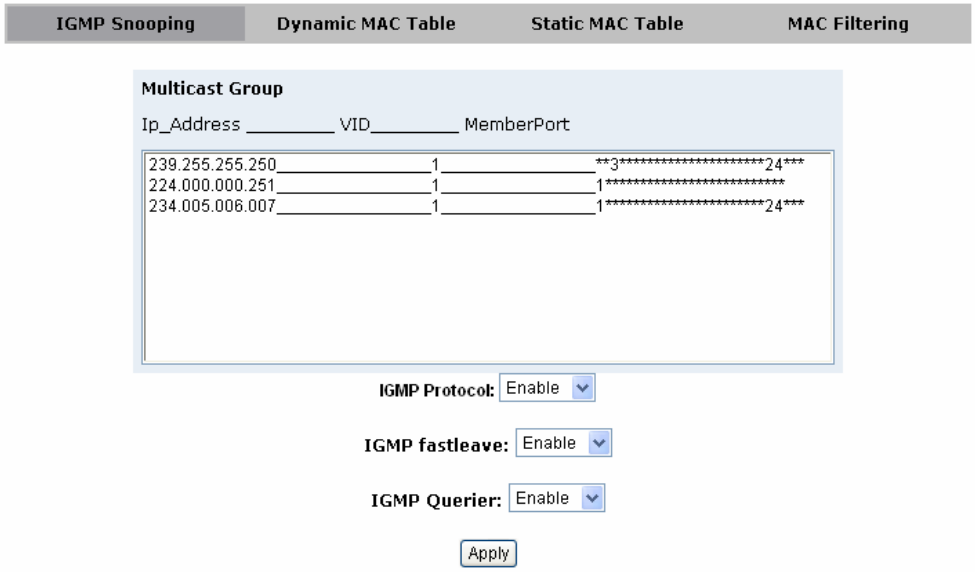
4.3.3 Forwarding and Filtering

In this submenu, the following functions related to forwarding and filtering are provided:

- IGMP Snooping
- Dynamic MAC Table
- Static MAC Table
- MAC Filtering

4.3.3.1 IGMP Snooping

This switch supports multicast IP; advanced settings can enable IGMP protocol on the switch of network management page, then display the IGMP snooping information in this page, you can view difference multicast group, VID and member port in here, IP multicast addresses range from 224.0.0.0 through 239.255.255.255.



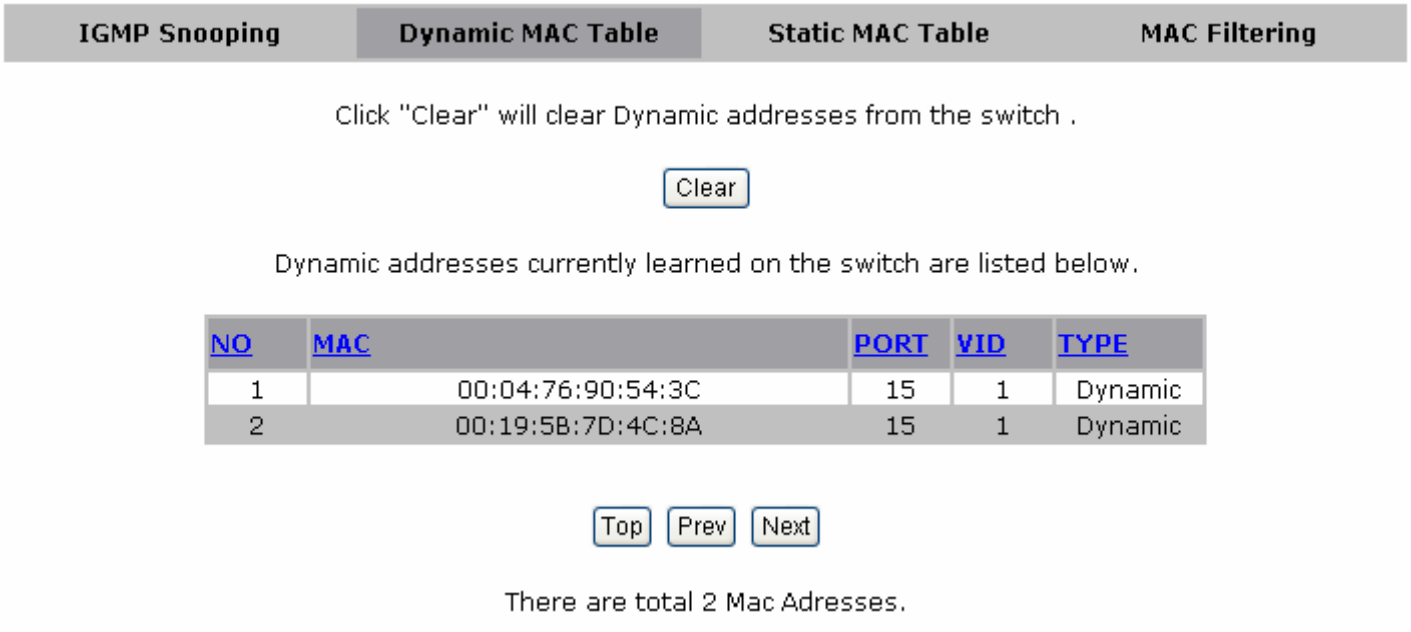
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.
IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the queries (IGMP router or switch) asking for a response from each host belonging multicast group.
Report	A message sent by a host to the queries to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the queries to indicate that the host has quit being a member of a specific multicast group.

IGMP protocol: Enable/disable IGMP snooping.
IGMP fast leave: Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report, else wait one second.
IGMP Querier: Enable/disable IGMP snooping querier. If select disable, the switch can't send query report.

4.3.3.2 Dynamic MAC Address

The switch will dynamically learn the device's MAC address when it corresponding with the switch. MAC address will be stored in MAC address table. Dynamic MAC Table shows the MAC addresses learned by the switch. The table will be shown by pages if larger than 500 MAC Addresses.



Click Clear to clear Dynamic MAC address table.

Click Top to show the first page of MAC address table.

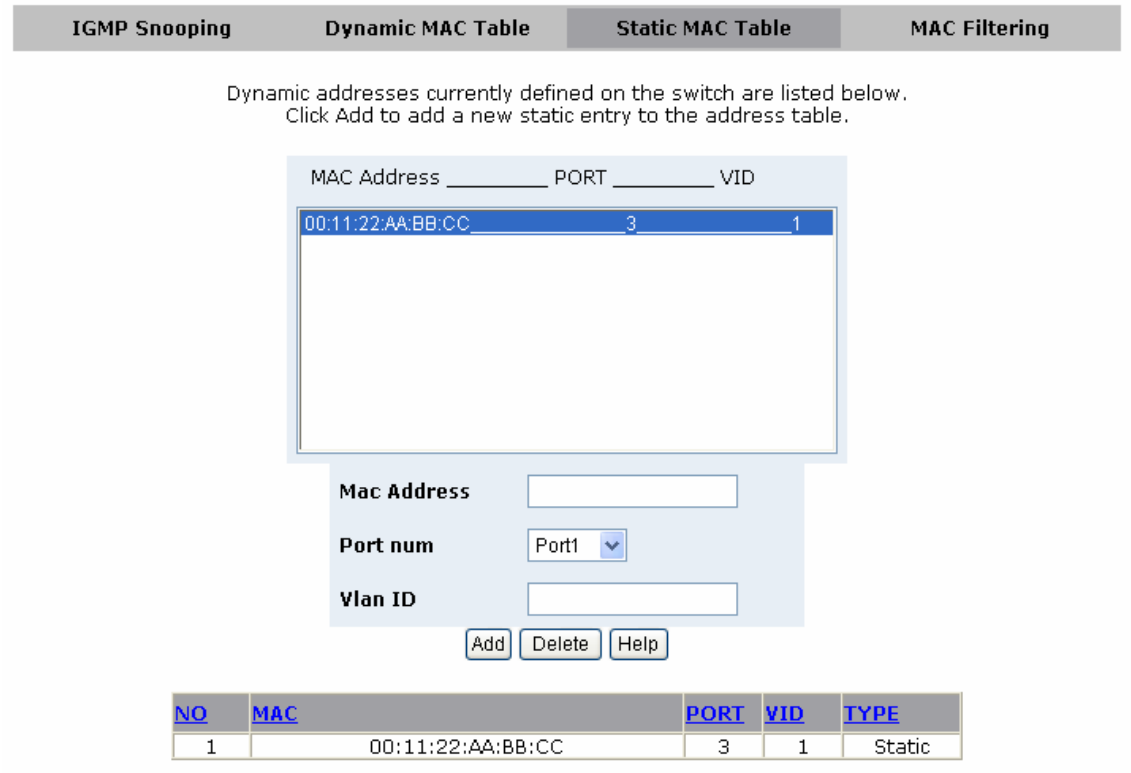
Click Prev to show the previous page of MAC address table. If there is nothing to shown or NO is 1, it is the first page.

Click Next to show the next page of MAC address table. If there is nothing to shown, it is the end page.

4.3.3.3 Static MAC Table

When you add a static MAC address, it permanently remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again.

This table can associate with the **Security** field in **Port Controls** configuration to achieve the access control by source MAC / port / VID binding. That is only ingress traffic with matched lookup (with specified MAC address, port number and VID) in this table can be allowed to access to the switch.



The following parameters can be associated to setup the Static MAC table:

MAC Address: Static MAC address in a MAC entry

Port number: Switch port number to associate with the MAC address in a MAC entry

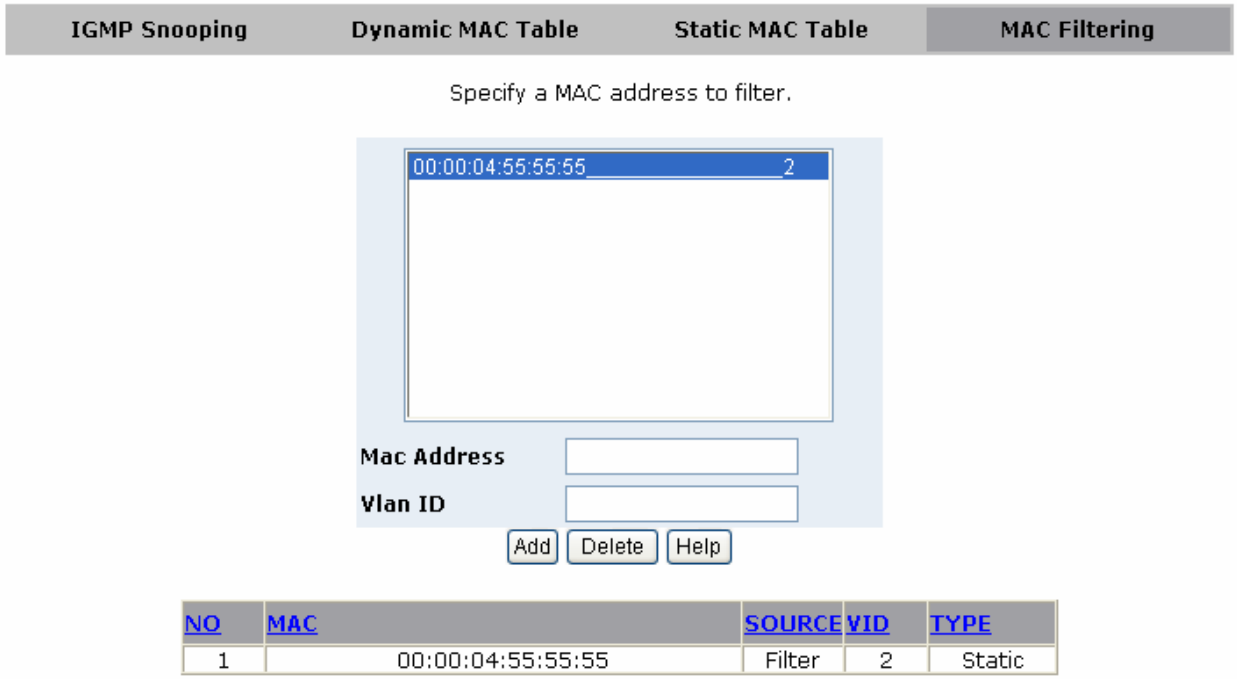
Vlan ID: If tag-based (IEEE 802.1Q) VLANs are enabled, static MAC address can be associated with individual VLANs. Type the VID in this field to associate with the MAC address.

Click Add to add a new entry. Click Delete to remove a specified entry.

The MAC entries in this table can be sorted by clicking the column NO / MAC / PORT / VID / TYPE.

4.3.3.4 MAC Filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination MAC addresses.



MAC Address: MAC address that wants to be filtered.

Vlan ID: If tag-based (802.1Q) VLAN are enabled, type the VID in this field to associate with the MAC address.

Click Add to add a new entry. Click Delete to remove a specified entry.

The MAC entries in this table can be sorted by clicking the column NO / MAC / PORT / VID / TYPE.

4.3.4 Spanning Tree

4.3.4.1 STP system

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1d) for avoiding loops in switching networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network. You can enable STP on web management's switch setting advanced item, select enable STP. We are recommended that you enable STP on all switches ensures a single active path on the network. You can view STP information about the Root Bridge. Such as following screen.

Root Bridge Information

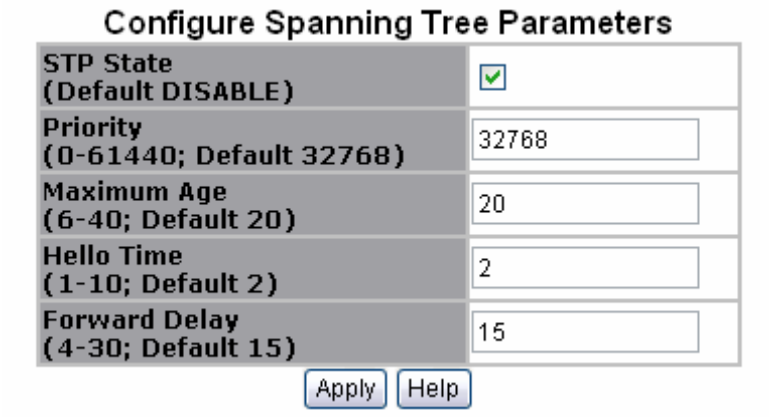
Priority	32768
MAC Address	00:00:24:15:17:67
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

You can view STP port status about the switch. Such as following screen.

STP Port Status

PortNum	PathCost	Priority	PortState
Port1	100	128	Disabled
Port2	100	128	Disabled
Port3	100	128	Disabled
Port4	19	128	Forwarding
Port5	100	128	Disabled
Port6	100	128	Disabled
Port7	100	128	Disabled
Port8	100	128	Disabled
Port9	100	128	Disabled
Port10	100	128	Disabled
Port11	100	128	Disabled
Port12	100	128	Disabled
Port13	100	128	Disabled
Port14	100	128	Disabled
Port15	100	128	Disabled
Port16	100	128	Disabled
Port17	100	128	Disabled
Port18	100	128	Disabled
Port19	100	128	Disabled
Port20	100	128	Disabled
Port21	100	128	Disabled
Port22	100	128	Disabled

You can configure STP parameters, then click Apply button to set the values. Such as following screen.



You can select STP state item to enable STP. If you want to disable STP, please cancel the item. Default value of STP sate is disabled.

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Value range <0-61440>, the value must be in steps of 4096. Default value is 32768.
Max Age	You can change Max Age value. The maximum age of received protocol information before it is discarded. Value range <6-40>. Default value is 20.
Hello Time	You can change Hello time value. The time interval between the transmission of Configuration BPDUs by a Bridge that is attempting to become the Root or is the Root. Value range <1-10>. Default value is 2.

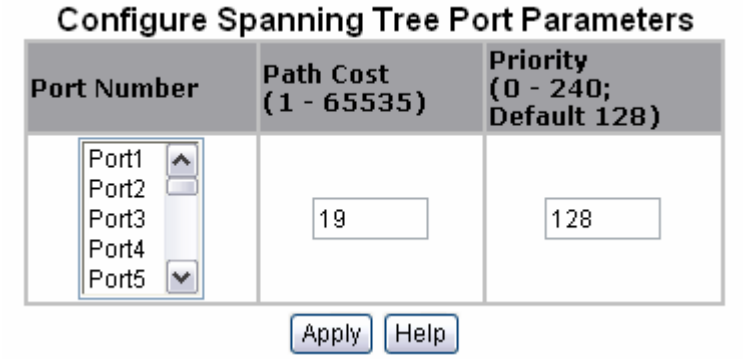
Forward Delay time	You can change forward delay time. The time spent by a Port in the Listening State and the Learning State before moving to the Learning or Forwarding State, respectively. It is also the value used for the ageing time of dynamic entries in the Filtering Database, while received BPDU indicate a topology change. Value range <4-30>. Default value is 15.

Note:

The above parameters must enforce the following relationships:

2*(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)

The following parameters can be configured on each port, click Apply button to set the values.



You can select one port in the Port Number item to configure the parameters of the port.

Parameter	Description
Path Cost	The contribution of the path through this port, when the port is the root port, to the total cost of the path to the root for this bridge. Value range <1-65535>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has the highest priority. Value range <0-240>, the value must be in steps of 16. Default value is128.

4.3.4.2 RSTP system

The Rapid Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.1W) that supersedes the Spanning Tree Algorithm and Protocol (STP) described as above and provides significantly faster reconfiguration. RSTP is compatible for STP, so the following content is mostly the same as the above STP description, adding some enhanced performance.
You can view RSTP information about the Root Bridge. Such as following screen.

Root Bridge Information

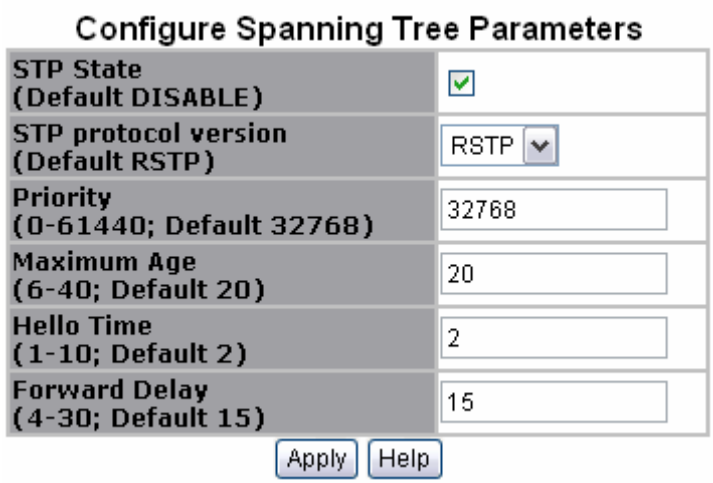
Priority	32768
MAC Address	00:00:24:15:17:67
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

You can view RSTP port status about the switch. Such as following screen.

STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	2000000	128	Disabled	NO	NO	NO
Port2	2000000	128	Disabled	NO	NO	NO
Port3	2000000	128	Disabled	NO	NO	NO
Port4	200000	128	Forwarding	NO	NO	YES
Port5	2000000	128	Disabled	NO	NO	NO
Port6	2000000	128	Disabled	NO	NO	NO
Port7	2000000	128	Disabled	NO	NO	NO
Port8	2000000	128	Disabled	NO	NO	NO
Port9	2000000	128	Disabled	NO	NO	NO
Port10	2000000	128	Disabled	NO	NO	NO
Port11	2000000	128	Disabled	NO	NO	NO
Port12	2000000	128	Disabled	NO	NO	NO
Port13	2000000	128	Disabled	NO	NO	NO
Port14	2000000	128	Disabled	NO	NO	NO
Port15	2000000	128	Disabled	NO	NO	NO
Port16	2000000	128	Disabled	NO	NO	NO
Port17	2000000	128	Disabled	NO	NO	NO
Port18	2000000	128	Disabled	NO	NO	NO
Port19	2000000	128	Disabled	NO	NO	NO
Port20	2000000	128	Disabled	NO	NO	NO
Port21	2000000	128	Disabled	NO	NO	NO

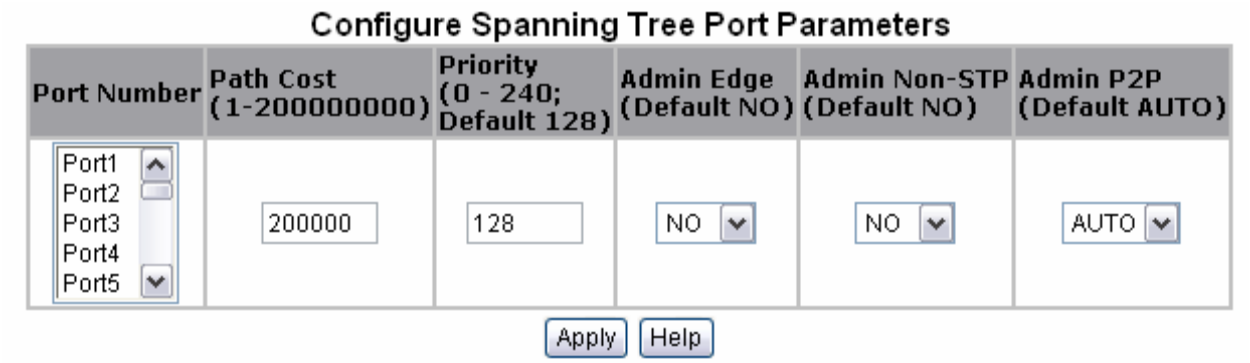
You can configure RSTP parameters, then click Apply button to set the values. Such as following screen.



Besides STP Debug and STP protocol version items, the remaining items are the same as STP describing above.
You can select STP Debug item to output RSTP debug information. If you want to disable the debug, please cancel the item. Default value of STP Debug is disabled.

STP protocol version item has two values for you to choose. If you want the protocol version to be STP, you can choose STP. If you want the protocol version to be RSTP, you can choose RSTP. Default value of STP protocol version is RSTP.

The following parameters can be configured on each port, click Apply button to set the values.



You can select one port in the Port Number item to configure the parameters of the port. Besides Path Cost and Priority items, the remaining items are newly enhanced performance. Priority item is just the same as STP, and the value range of Path Cost item is different from STP.

Parameter	Description
Path Cost	The contribution of the path through this port, when the port is the root port, to the totalcost of the path to the root for this bridge. Value range <1-200000000>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has thehighest priority. Value range <0-240>, the value must be in steps of 16. Default value is 28.
Admin Edge	You can choose the value of YES if you want the port to be edge port. If the port is edgeport, when the port becomes a Designated Port it can rapidly transition to the Forwarding Port State. Value range <NO | YES>. Default

	value is NO.
Admin Non -STP	If you want to disable spanning tree protocol on the port, you can choose the value of YES to this port. Value range <NO | YES>. Default value is NO.
Admin P2P	If you want point-to-point link auto detection on the port, you can choose the value of AUTO to this port. If you want point-to-point link of the port always be true, you can choose the value of YES to this port. If you want point-to-point link of the port always be false, you can choose the value of NO to this port. Value range <AUTO | NO | YES>.Default value is AUTO.

4.3.4.3 MSTP system

The Multiple Spanning Tree Protocol (MSTP) is a standardized method (IEEE 802.1S) for providing simple and full connectivity for frames assigned to any given VLAN throughout a Bridged Local Area Network comprising arbitrarily interconnected Bridges, each operating MSTP, STP , or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. These Regions and the other Bridges and LANs are connected into a single Common Spanning Tree (CST).
You can enable MSTP on web management's switch setting advanced item, select enable MSTP. We are recommended that you enable MSTP on all switches ensures a single active path on the network.

You can view MSTP information about the CIST Root Bridge. Such as following screen.

Root Bridge Information

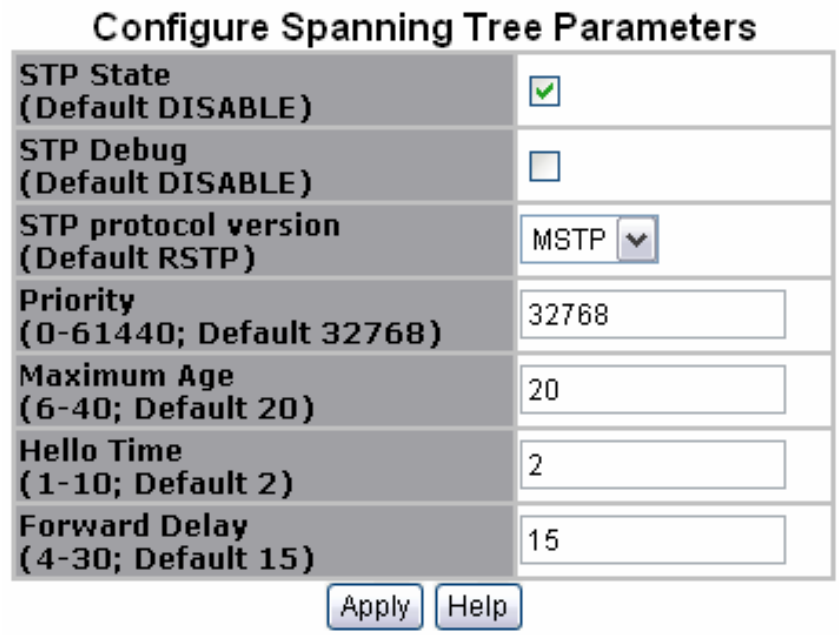
Priority	32768
MAC Address	00:00:24:15:17:67
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

You can view MSTP CIST port status about the switch. Such as following screen

STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	2000000	128	Disabled	NO	NO	NO
Port2	2000000	128	Disabled	NO	NO	NO
Port3	2000000	128	Disabled	NO	NO	NO
Port4	200000	128	Forwarding	NO	NO	YES
Port5	2000000	128	Disabled	NO	NO	NO
Port6	2000000	128	Disabled	NO	NO	NO
Port7	2000000	128	Disabled	NO	NO	NO
Port8	2000000	128	Disabled	NO	NO	NO
Port9	2000000	128	Disabled	NO	NO	NO
Port10	2000000	128	Disabled	NO	NO	NO
Port11	2000000	128	Disabled	NO	NO	NO
Port12	2000000	128	Disabled	NO	NO	NO
Port13	2000000	128	Disabled	NO	NO	NO
Port14	2000000	128	Disabled	NO	NO	NO
Port15	2000000	128	Disabled	NO	NO	NO
Port16	2000000	128	Disabled	NO	NO	NO
Port17	2000000	128	Disabled	NO	NO	NO
Port18	2000000	128	Disabled	NO	NO	NO
Port19	2000000	128	Disabled	NO	NO	NO
Port20	2000000	128	Disabled	NO	NO	NO
Port21	2000000	128	Disabled	NO	NO	NO

You can configure MSTP parameters, then click Apply button to set the values. Such as following screen.



You can select STP state item to enable MSTP. If you want to disable MSTP, please cancel the item. Default value of STP sate is disabled.

You can select STP Debug item to output MSTP debug information. If you want to disable the debug, please cancel the item. Default value of STP Debug is disabled.

STP protocol version item has two values for you to choose. If you want the protocol version to be STP, you can choose STP. If you want the protocol version to be MSTP, you can choose MSTP. Default value of STP protocol version is MSTP.

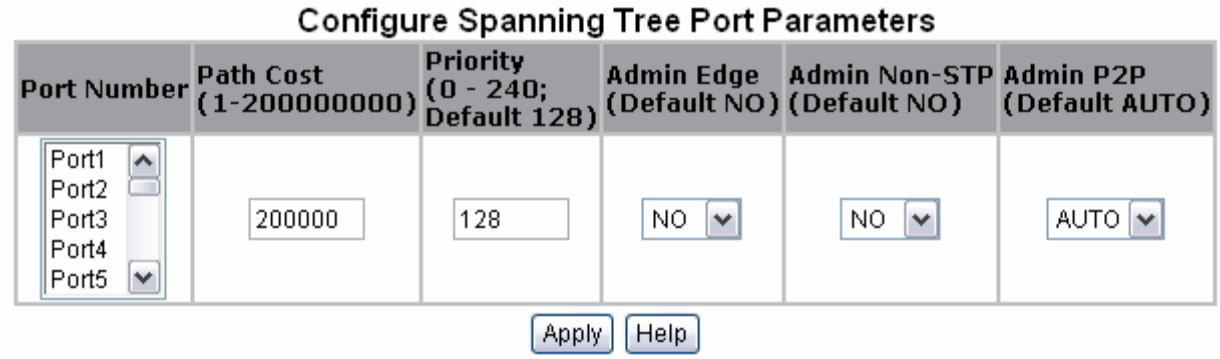
Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Value range <0-61440>, the value must be in steps of 4096. Default value is 32768.
Max Age	You can change Max Age value. The maximum age of received protocol information before it is discarded. Value range <6-40>. Default value is 20.
Hello Time	You can change Hello time value. The time interval between the transmission of Configuration BPDUs by a Bridge that is attempting to become the Root or is the Root. Value range <1-10>. Default value is 2.
Forward Delay time	You can change forward delay time. The time spent by a Port in the Listening State and the Learning State before moving to the Learning or Forwarding State, respectively. It is also the value used for the ageing time of dynamic entries in the Filtering Database, while received BPDU indicate a topology change. Value range <4-30>. Default value is 15.

Note:

The above parameters must enforce the following relationships:

2*(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)

The following parameters can be configured on each CIST port, click Apply button to set the values.



You can select one port in the Port Number item to configure the parameters of the CIST port.

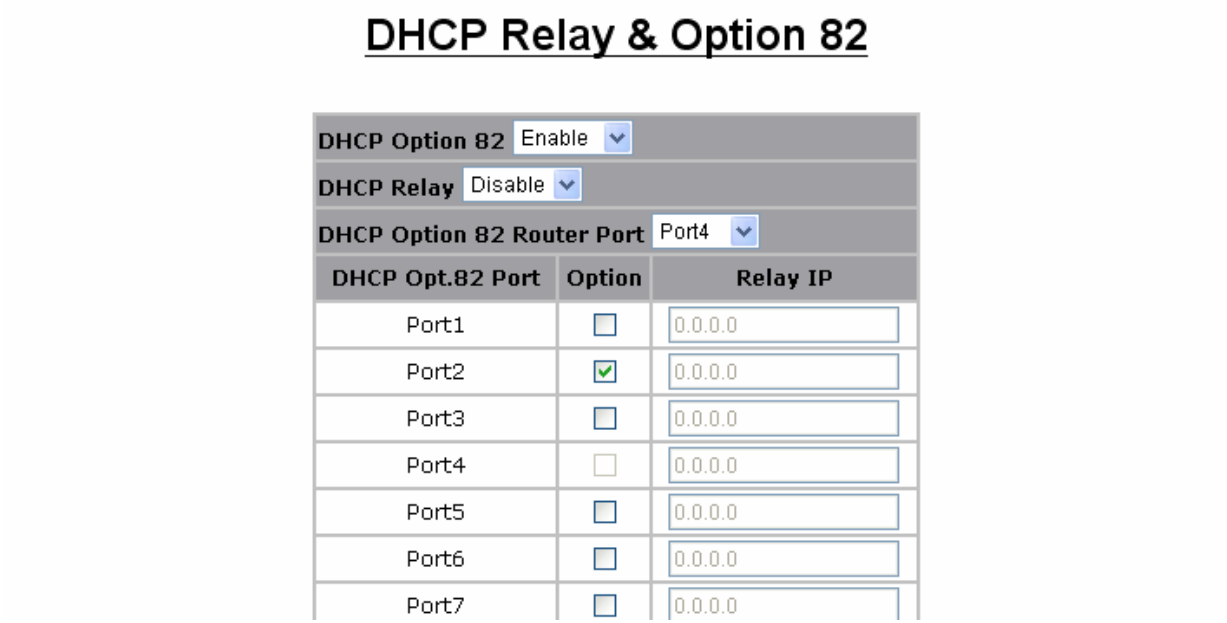
Parameter	Description
Path Cost	The contribution of the path through this port, when the port is the root port, to the totalcost of the path to the root for this bridge. Value range <1-200000000>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has thehighest priority. Value range <0-240>, the value must be in steps of 16. Default value is 28.
Admin Edge	You can choose the value of YES if you want the port to be edge port. If the port is edgeport, when the port becomes a Designated Port it can rapidly transition to the Forwarding Port State. Value range <NO | YES>. Default value is NO.
Admin Non -STP	If you want to disable spanning tree protocol on the port, you can choose the value of YES to this port. Value range <NO | YES>. Default value is NO.
Admin P2P	If you want point-to-point link auto detection on the port, you can choose the value of AUTO to this port. If you want point-to-point link of the port always be true, you can choose the value of YES to this port. If you want point-to-point link of the port always be false, you can choose the value of NO to this port. Value range <AUTO | NO | YES>.Default value is AUTO.

4.3.5 DHCP Relay and Option 82

The Relay Agent Information option (Option82) is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The DHCP Relay can forward the DHCP broadcast packets to a DHCP server in a different subnet (RFC 1542). So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

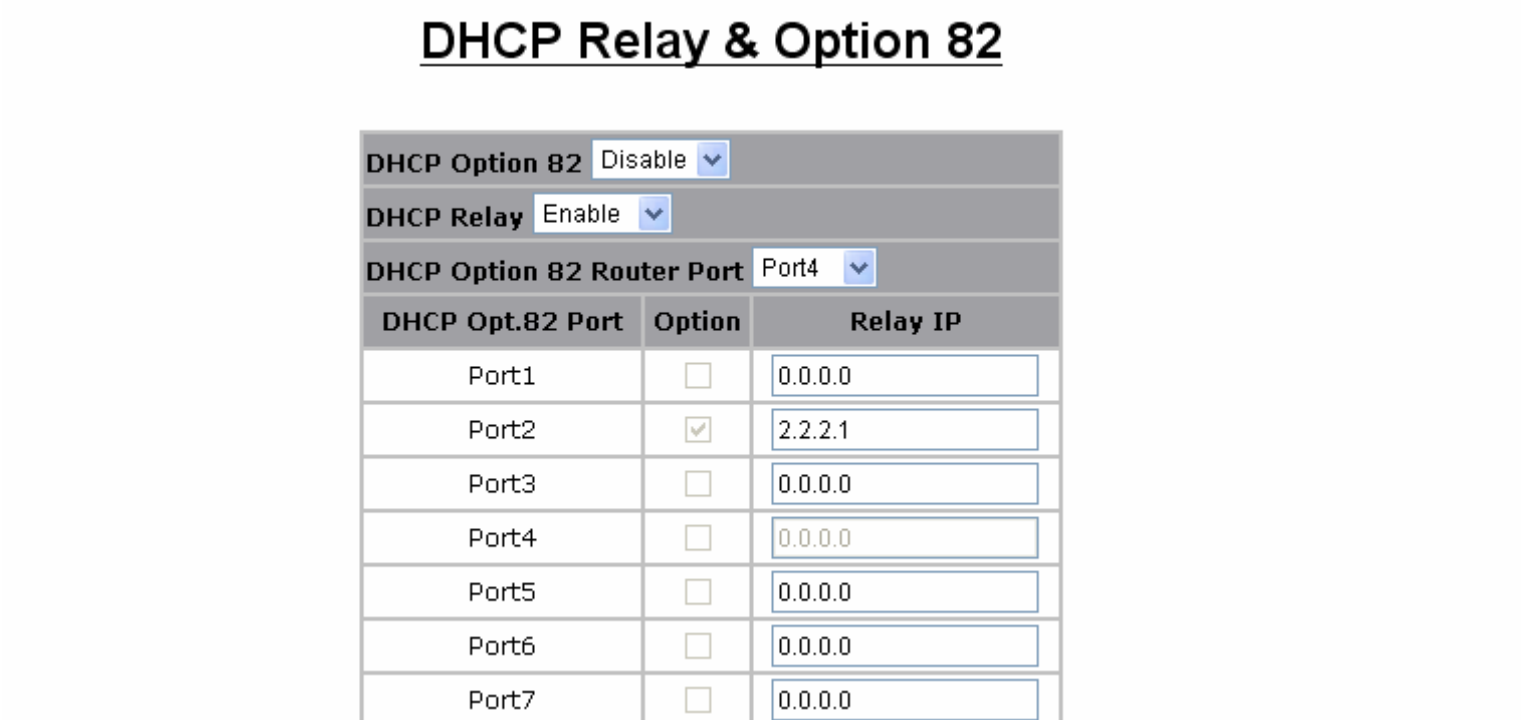
4.3.5.1DHCP Option82

To enable DHCP option82 function, need to enable global option82 and special port option82. Then select DHCP router port.



4.3.5.2 DHCP Relay

To enable DHCP relay function, need to enable global dhcp-relay and special port dhcp-relay. Then select DHCP router port.

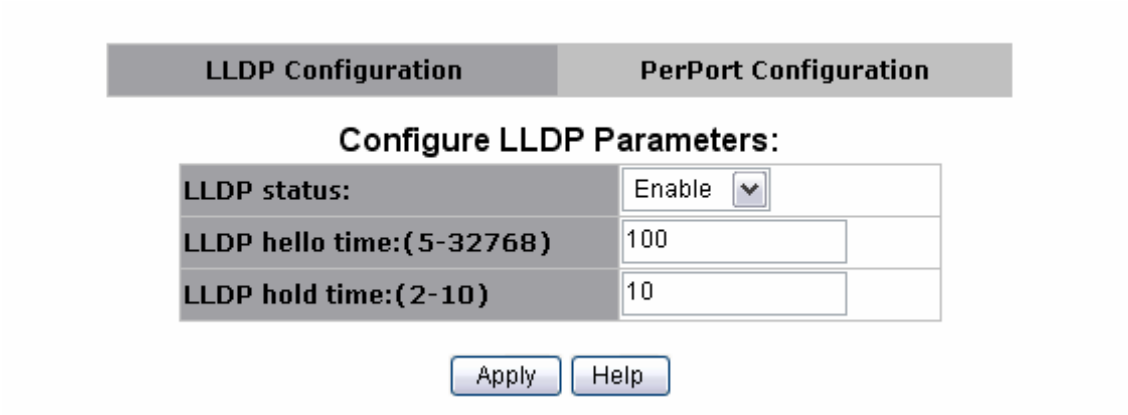


4.3.6 LLDP

This switch supports LLDP (Link Layer Discovery Protocol) function. Please refer to the section 4.3.7 which has descriptions about the LLDP function and operation in console. Here is the web UI to configure this function.

4.3.6.1 LLDP Configuration

This page is to provide the global parameters for LLDP for configuration.



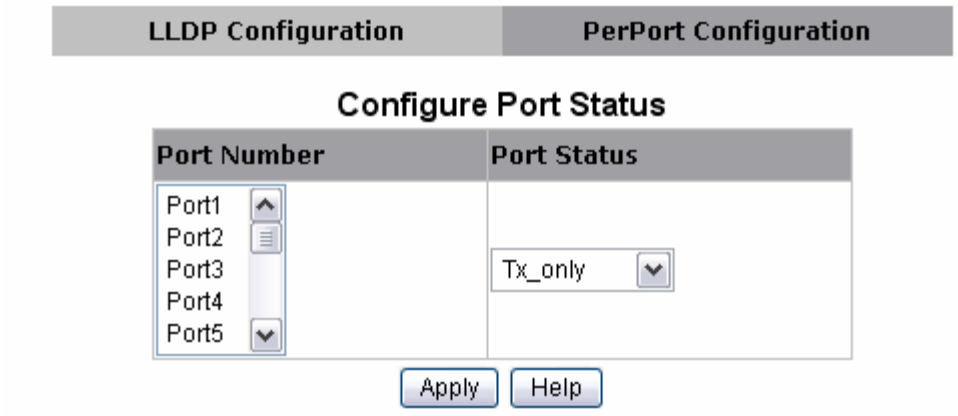
LLDP Status: Enable/Disable LLDP.
LLDP hello time: LLDP hello time value which is time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.
LLDP hold time: LLDP hold time value. Value range is from 2 to 10. Default value is 4.

TTL (time to live) is a period of time for keeping the information about a neighboring device. The information will be aged out

when the corresponding TTL expires. TTL can be calculated by configuring LLDP hello time and hold time according to the following expression:
TTL = LLDP hello time × LLDP hold time

4.3.6.2 PerPort Configuration

PerPort LLDP configuration is in this page:



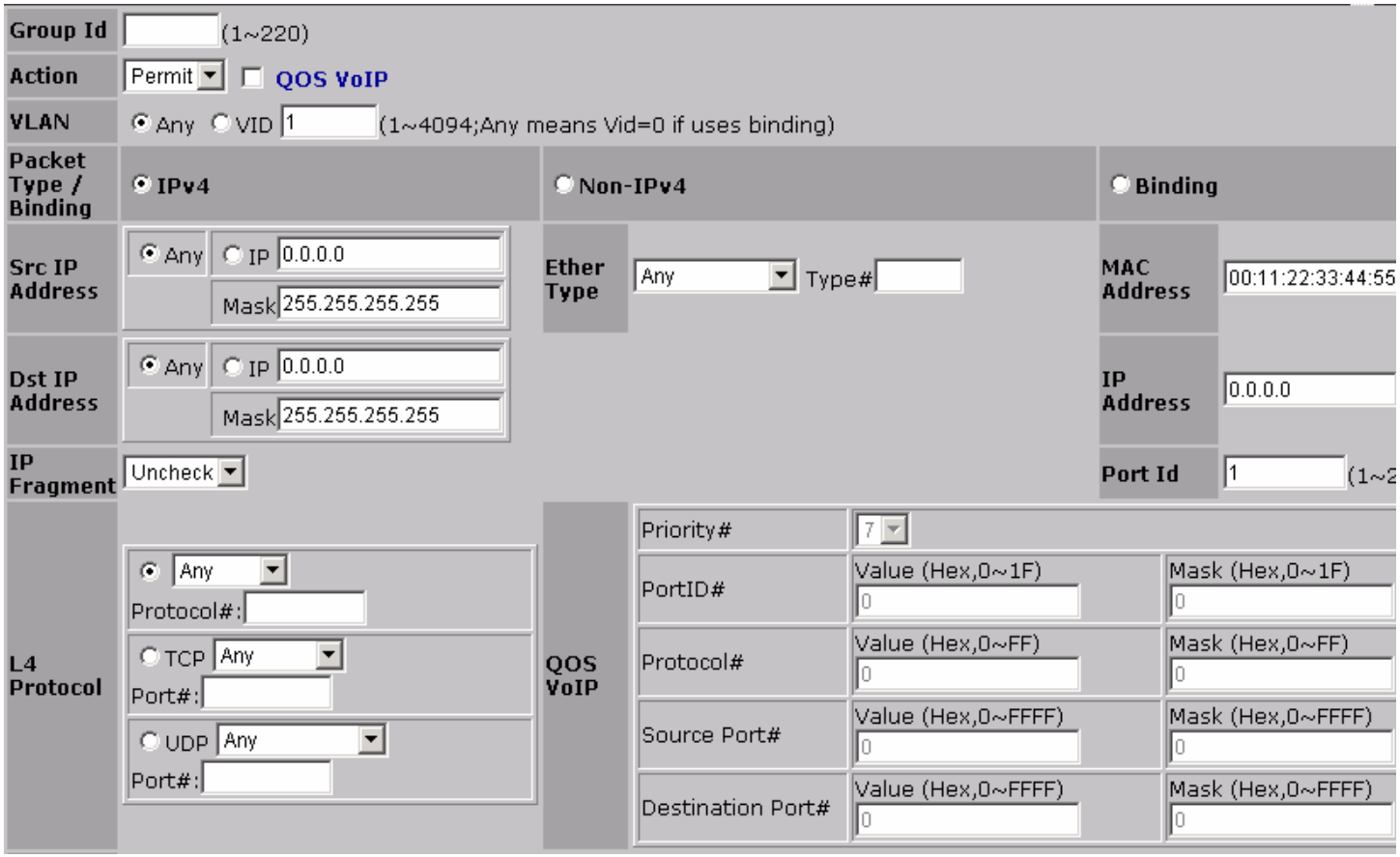
Port Number: specify the port(s) to be configured in the switch.
Port Status: specify one of four port mode to operate LLDP for specified port(s)
Tx_only: LLDP transmit the packet of the port only
Rx_only: LLDP receive the packet of the port only.
Tx_and_Rx: LLDP transmit and receive the packets of the port.
Disable: LLDP do not transmit and receive the packets of the port.
PerPort LLDP configuration status can be shown in the lower area of this page like the following example:

Port Status

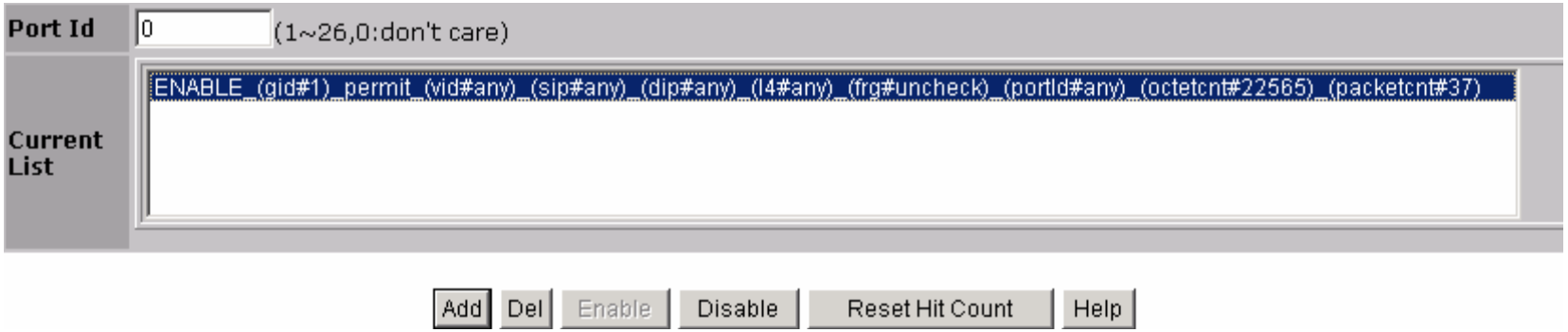
PortNum	Status
Port1	Tx_only
Port2	Tx_only
Port3	Tx_and_Rx
Port4	Tx_and_Rx
Port5	Rx_only
Port6	Rx_only
Port7	Disable
Port8	Disable
Port9	Tx_and_Rx
Port10	Tx_and_Rx
Port11	Tx_and_Rx
Port12	Tx_and_Rx
Port13	Tx_and_Rx
Port14	Tx_and_Rx
Port15	Tx_and_Rx
Port16	Tx_and_Rx
Port17	Tx_and_Rx

4.4 Access Control List

Packets can be forwarded or dropped by ACL rules include IPv4 or non-Ipv4. VT6530 can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.



There are 2 main ACL rule types to setup: **Packet Type** (IPv4 and Non-IPv4) and **Binding** (SIP-SMAC-Port).

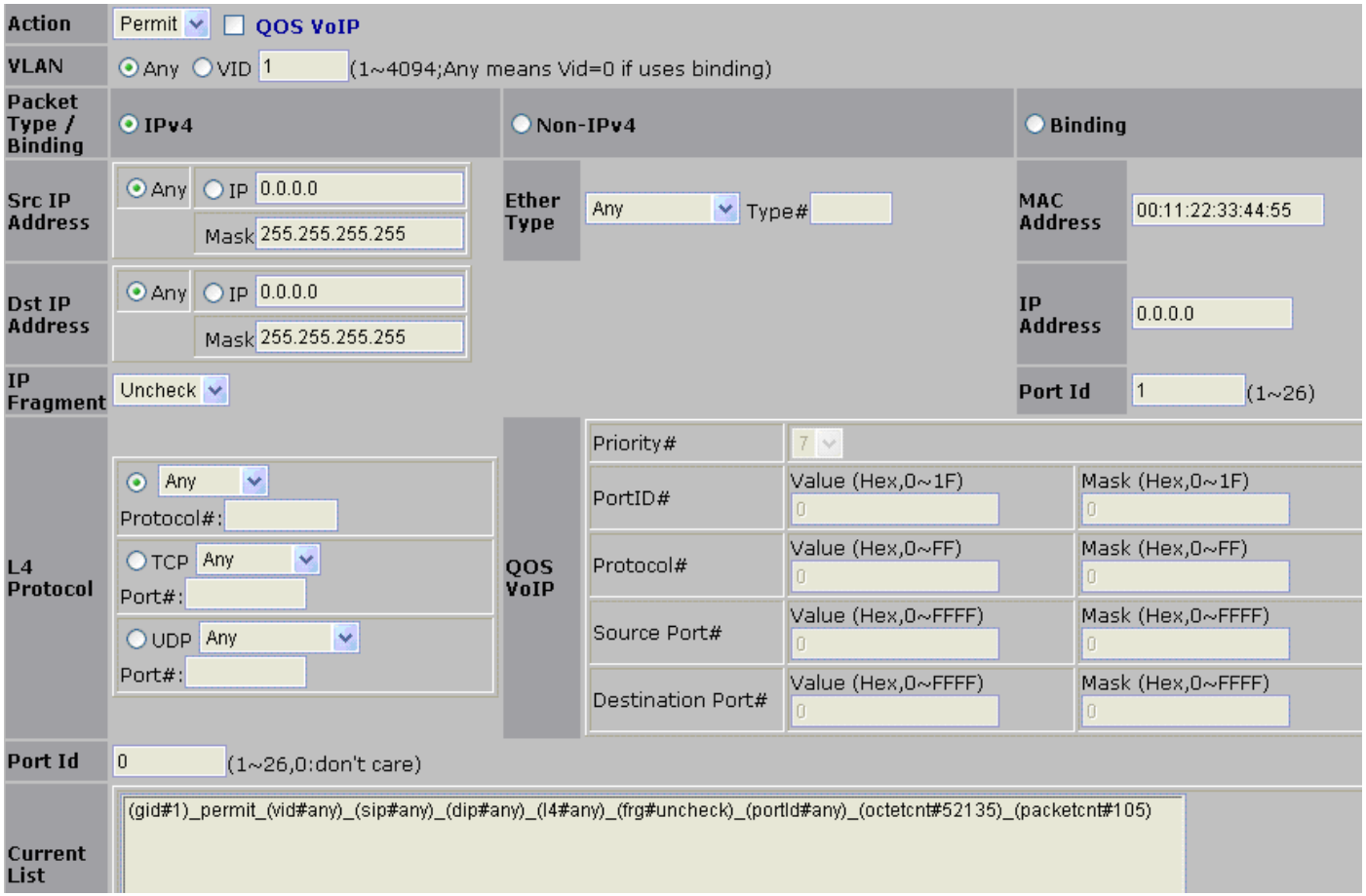


Enable/Disable ACL rule: Select an ACL entry which you want to enable/disable in the Current List. Then click Enable / Disable to execute.

Reset ACL count: Select an ACL entry which you want to reset its counts (**octetcnt** and **packetcnt** fields) in the Current List. Then click Reset Hit Count to do the action.

4.4.1 IPv4

In "Packet Type / Binding" box should select "IPv4".



The related parameters are shown in the following table:

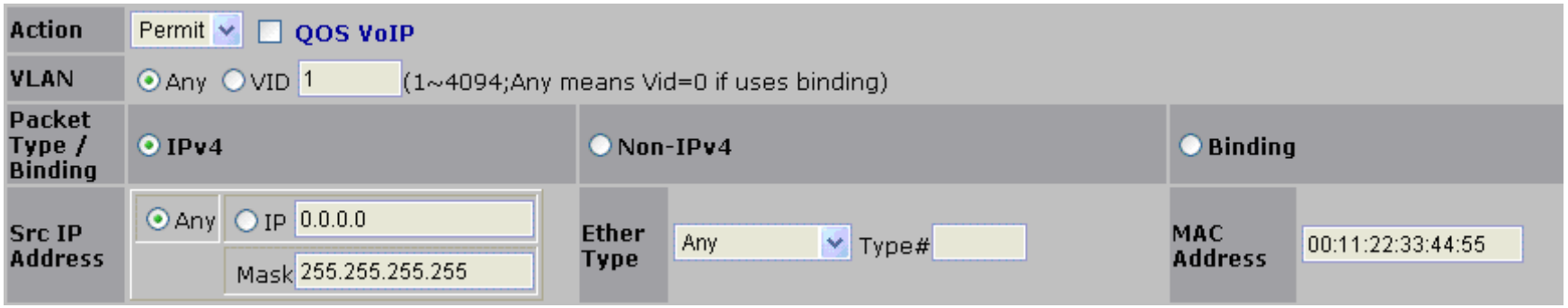
Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. a. Permit : Permit packet cross switch. b. Deny: Drop packet.	**Permit**
VLAN	Any / VID. a. Any: Any Vlan id. b. VID: 1~4094. A certain vlan id.	**Any**
Packet Type	IPv4 / Non-IPv4 / Binding a. IPv4: Set Ipv4 packet field. b. Non-IPv4: Set non-Ipv4 packet field. c. Binding: Set binding entry.	**IPv4**
Src IP Address	(Set this field if Packet Type is IPv4, else ignore.) Any / IP and Mask a. Any: Any IP address. b. IP :A certain IP address. Mask: ***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255 **Notice: This is not subnet mask.**	**Any**

Dst IP Address	(Set this field if Packet Type is IPv4, else ignore.) Any / IP and Mask a. Any: Any IP address. b. IP :A certain IP address. Mask: ***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255	**Any**
IP Fragment	(Set this field if Packet Type is IPv4, else ignore.) Uncheck / Check a. Uncheck: Not check IP fragment field. b. Check: Check IP fragment field.	**Uncheck**
L4 Protocol	(Set this field if Packet Type is IPv4, else ignore.) Any / ICMP(1) / IGMP(2) / TCP(6) / UDP(17)	**Any**
Protocol	(Set this field if Packet Type is IPv4, else ignore.) 0~255. If protocol not find in **L4 Protocol field, you can direct assign number.**	
TCP	(Set this field if Packet Type is IPv4, else ignore.) Any / FTP(21) / HTTP(80)	**Any**

Port	(Set this field if Packet Type is IPv4, else ignore.) 0~65535 If TCP port not find in TCP field, you can direct assign number.	
UDP	(Set this field if Packet Type is IPv4, else ignore.) Any / DHCP(67) / TFTP(69) / NetBios(137)	**Any**
Port	(Set this field if Packet Type is IPv4, else ignore.) 0~65535 If UDP port not find in **UDP field, you can direct assign number.**	
Port Id	Source port id, from 1~26, 0 means don't care.	**0**
Current List	You create ACL and Binding groups.	
Count	The octetcnt is octet number of the packets hiting the ACL rule. The packetcnt is the packet number Hiting the ACL rule.	**0**

4.4.2 Non-IPv4

In "Packet Type / Binding" box should select "Non-IPv4".



The related parameters are shown in the following table:

Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. c. Permit : Permit packet cross switch. d. Deny: Drop packet.	**Permit**
VLAN	Any / VID. a. Any: Any Vlan id. b. VID: 1~4094. A certain vlan id.	**Any**

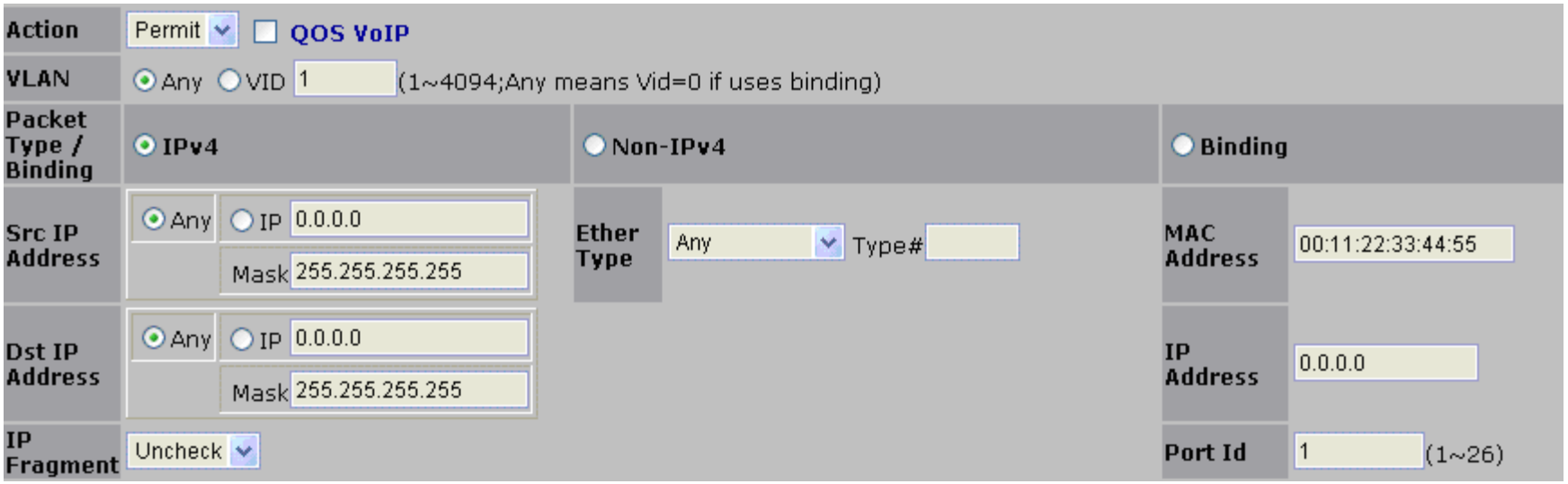
Packet Type	IPv4 / Non-IPv4 / Binding d. IPv4: Set Ipv4 packet field. e. Non-IPv4: Set non-Ipv4 packet field. f. Binding: Set binding function.	**IPv4**
Ether Type	(Set this field if Packet Type is Non-IPv4, else ignore.) Any / ARP(0x0806) / IPX(0x8137)	**Any**
Type	(Set this field if Packet Type is Non-IPv4, else ignore.) 0~0xFFFF If ether type not find in Ether Type field, you can direct assign number.	
Current List	You create ACL and Binding groups.	

4.4.3 Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN id and port id to bind, and device can cross switch if all conditions match.

Use binding function; we should enable it first in following page.

In "Packet Type / Binding" box should select "Binding".



The related parameters are shown in the following table:

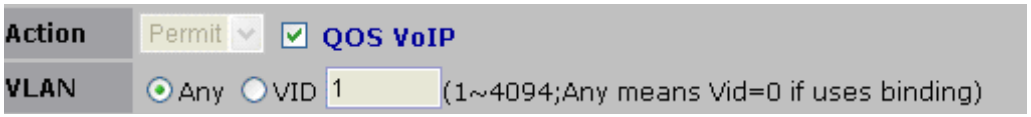
Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. e. Permit : Permit packet cross switch. f. Deny: Drop packet.	**Permit**
VLAN	Any / VID. e. Any: Any Vlan id. f. VID: 1~4094. A certain vlan id.	**Any**
Packet Type	IPv4 / Non-IPv4 / Binding g. IPv4: Set Ipv4 packet field. h. Non-IPv4: Set non-Ipv4 packet field. i. Binding: Set binding function.	**IPv4**
Mac address	**:**:**:**:**:** * is represent a digit from 0~9 and A~F, *** is range from 0 to FF.	**00:11:22:33:44:55**
IP address	***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255.	**0.0.0.0**
Port Id	Source port id, from 1~26.	**1**
Current List	You create ACL and Binding groups.	

4.4.4 QoS VoIP

QoS VoIP option in Action field is to provide ingress VoIP packets can be forwarded out with higher priority through the ACL function.

QoS VoIP option in Action field is to provide ingress VoIP packets can be forwarded out with higher priority through the ACL function.

In "Action" box select the "QoS VoIP" checkbox to make QoS VoIP parameter area available to configure.



QoS VoIP Parameter	Option	Default value
Priority	**0 ~ 7**	7
PortID	**0~1F**	**0**
PortID Mask	**0~1F**	**0**
Protocol	**0~FF**	**0**
Protocol Mask	**0~FF**	**0**
Source Port	**0~FFFF**	**0**
Source Port Mask	**0~FFFF**	**0**
Destination Port	**0~FFFF**	**0**
Destination Port Mask	**0~FFFF**	**0**

All parameters with HEX format provide settings in continuous range.

For example, if we want VoIP packets, with UDP protocol type (17) and source port number is in range of 10000~10015, to be forwarded out with highest priority while network congestion happens, an ACL rule can be created like the following setting:

Parameter	Value
GID	1
Action	QoS VoIP
VLAN	Any
Priority	7
PortID	0
PortID Mask	0
Protocol	11h
Protocol Mask	1FH
Source Port	2710h
Source Port Mask	FF00h
Destination Port	0
Destination Port Mask	0

4.5 Security

4.5.1 Security Manager

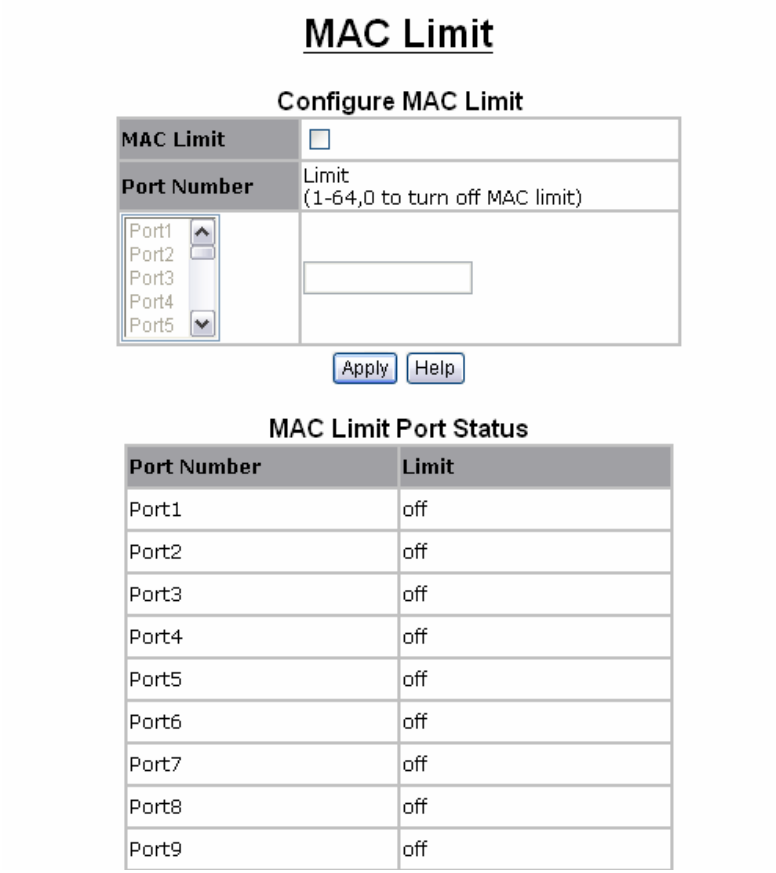
In this page, user can change user name and password with the following parameters.

User Name: Type the new user name.
Assign/Change password: Type the new password.
Reconfirm password: Retype the new password.

Click Apply to activate the setting.

4.5.2 MAC Limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.



MAC Limit: enable/disable MAC limit function

Limit: select port number and input Limit value (0~64, 0 to turn off MAC limit)

Click Apply to activate the setting.

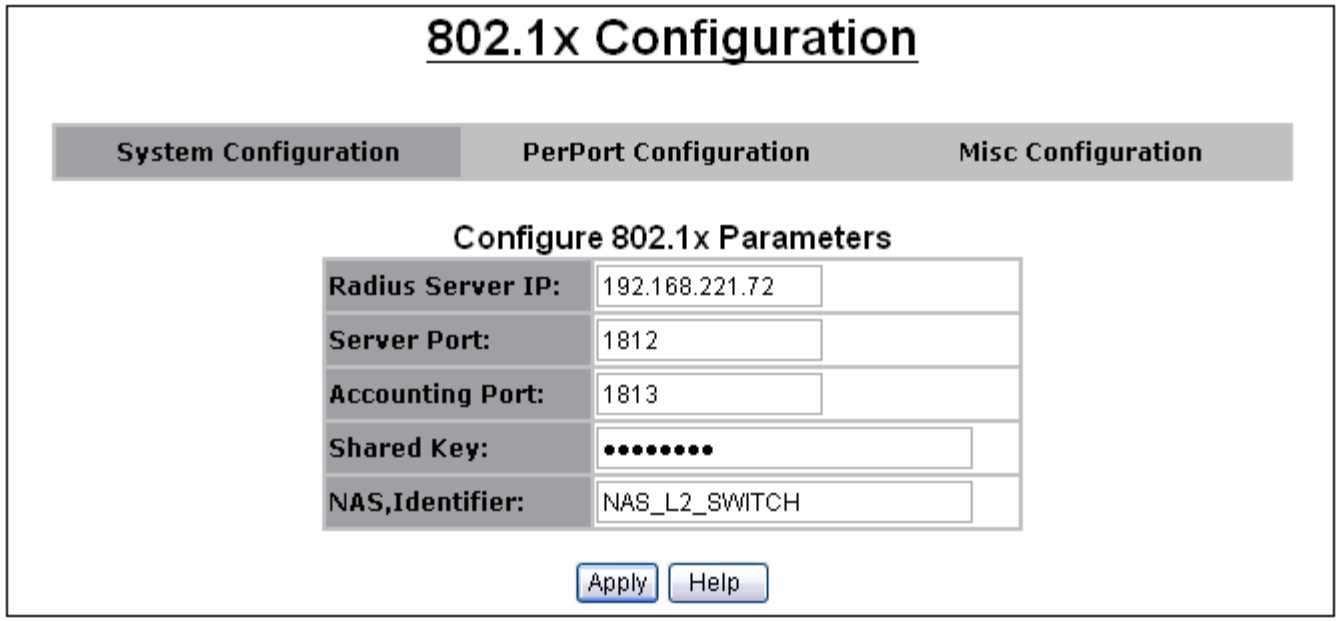
4.5.3 802.1x Configuration

802.1x makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

In the beginning, 802.1x configuration page is disabled because 802.1x is disabled in default. To enable 802.1x, go to **Administration** ->**Switch setting** ->**Misc Configs** page to enable the **802.1x protocol** field. After clicked Apply, the 802.1x configuration page will be shown up.

4.5.3.1 System Configuration

In this page, the parameters related to authentication (Radius) server are provided:



Radius Server IP: the IP address of the authentication server.

Server Port: The UDP port number used by the authentication server to authenticate (default: 1812).

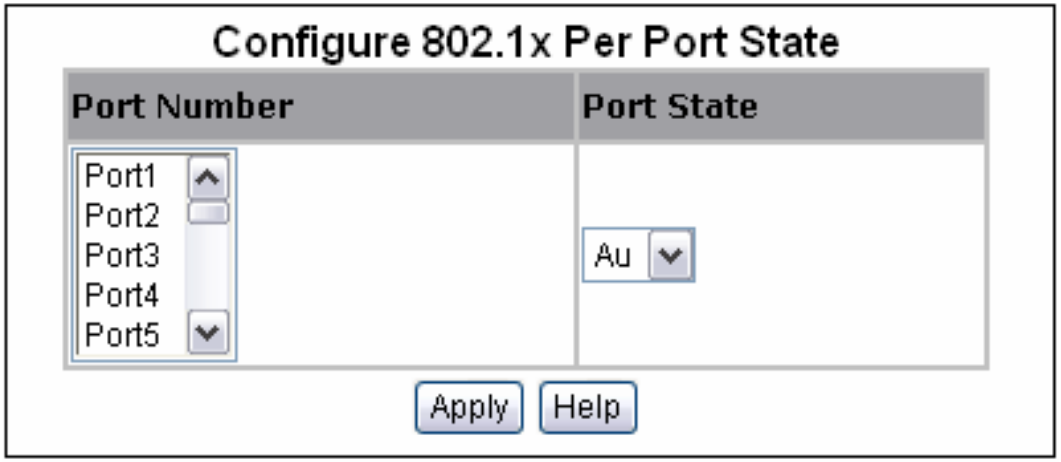
Accounting Port: The UDP port number used by the authentication server to retrieve accounting information (default: 1813).

Shared Key: A key shared between this switch and authentication server.

NAS, Identifier: A string used to identify this switch.

4.5.3.2 Perport Configuration

In this page, you can select the specific port and configure the authorization state. There are 4 kinds of authorization state to provide for each port.



Fu: Force the specific port to be unauthorized.

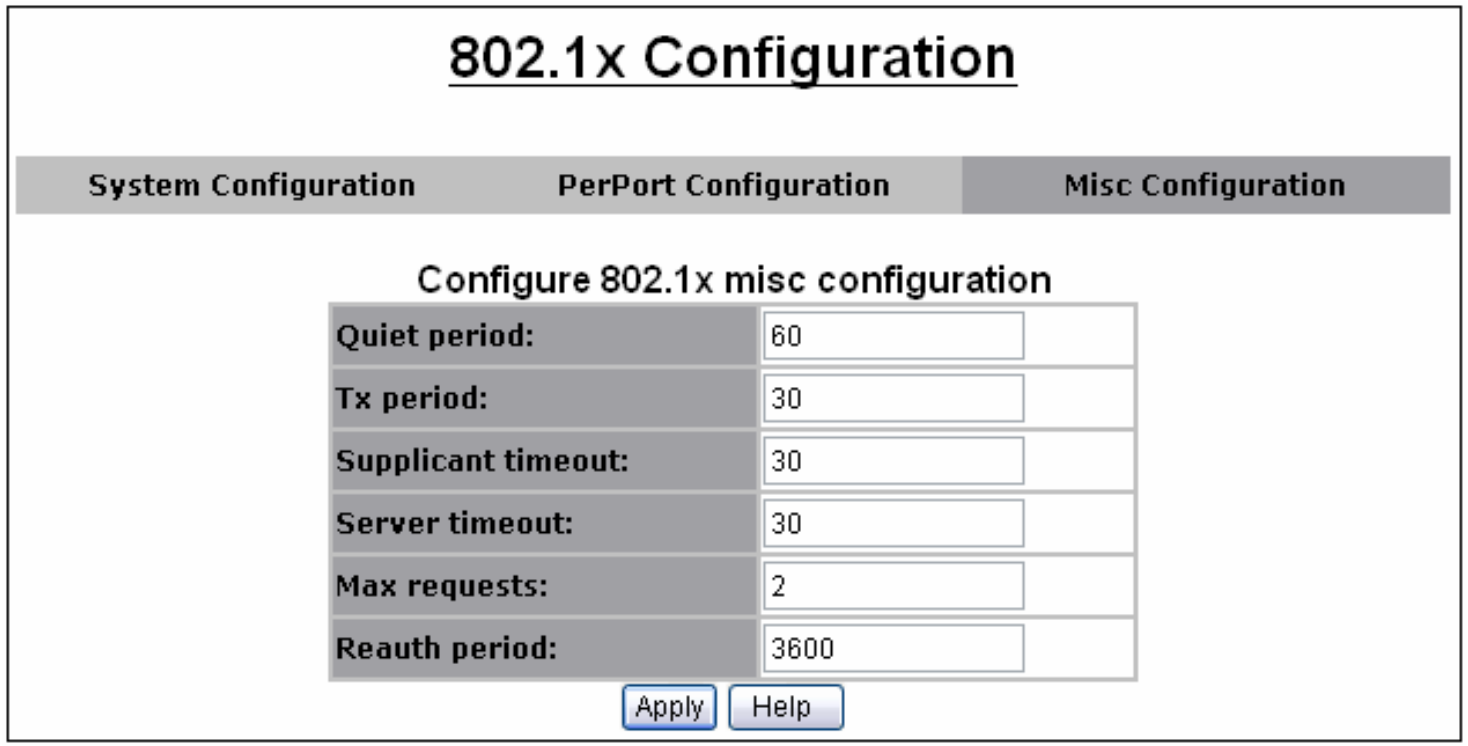
Fa: Force the specific port to be authorized.

Au: The state of the specific port was determined by the outcome of the authentication.

No: The specific port didn't support 802.1x function.

4.5.3.3 Misc Configuration

In this page, you can change the default configuration for the 802.1x standard:



Quiet Period: Used to define periods of time during which it will not attempt to acquire a supplicant (default time: 60 seconds).

Tx Period: Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).

Supplicant Timeout: Used to determine timeout conditions in the exchanges between the supplicant and authentication server (default value: 30 seconds).

Server Timeout: Used to determine timeout conditions in the exchanges between the authenticator and authentication server

(default value: 30 seconds).

ReAuthMax: Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (default value: 2 times).

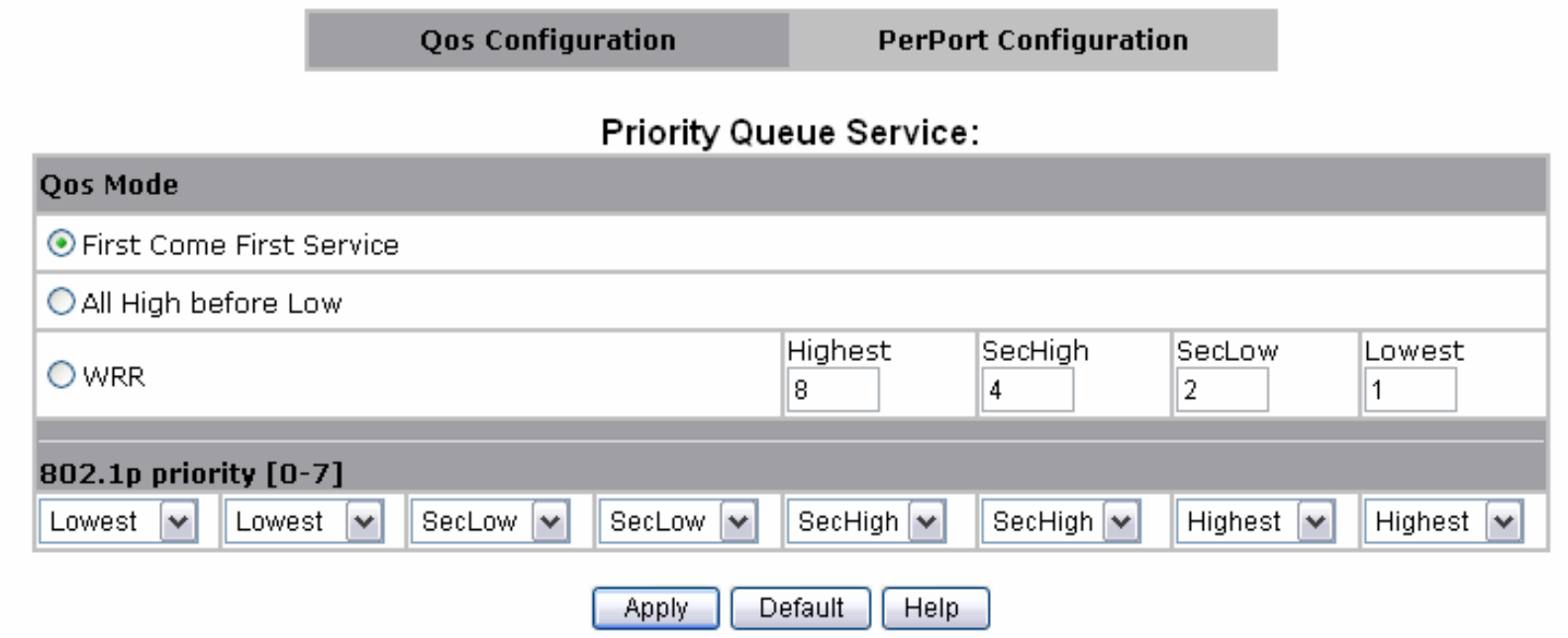
Reauth Period: Used to determine a nonzero number of seconds between periodic re-authentication of the supplications (default value: 3600 seconds).

4.6 QoS

This switch provides quality of service (QoS) to prioritize the packet forwarding when traffic congestion happens. This switch supports port-based (4-level output queue) and 802.1p (8-level priority to 4-level queue mapping) QoS functions. Strict and weight round robin (WRR) QoS mode are supported.

4.6.1 QoS Configuration

This page is mainly to set the QoS mode (First Come First Service, All High before Low, and WRR) and 8-level priority to 4 – level queue mapping.



First Come First Service: The sequence of packets sent is depending on arrive orders. This mode can be regarded as QoS is

disabled.

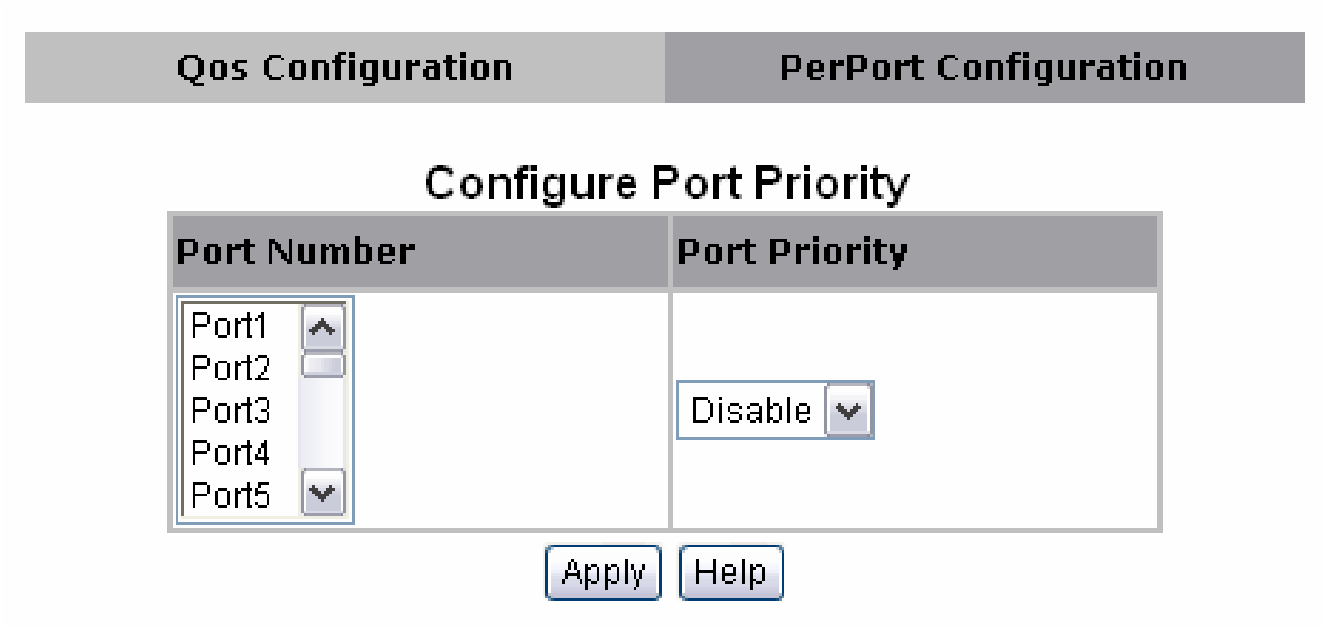
All High before Low: The high priority packets sent before low priority packets.

WRR: Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest：4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.

QoS Priority: 8-level (0~7) priority can be mapped to 4-level (Highest, Second-High, Second-Low, Lowest) queue.

4.6.2 Per-Port Configuration

Per-port priority can be configured and shown in this page.



Port Number: the ports in the switch.

Port Priority: port priority can be disable or 0-7.

Per-Port priority setting can be displayed like the following figure.

Port Priority

PortNum	Priority
Port1	Disable
Port2	Disable
Port3	Disable
Port4	Disable
Port5	Disable
Port6	Disable
Port7	Disable
Port8	Disable
Port9	Disable
Port10	Disable
Port11	Disable
Port12	Disable
Port13	Disable
Port14	Disable
Port15	Disable
Port16	Disable
Port17	Disable
Port18	Disable
Port19	Disable
Port20	Disable
Port21	Disable
Port22	Disable
Port23	Disable
Port24	Disable

4.7 Monitoring

The following items are provided in Monitoring section:

- Port status
- Port statistics

4.7.1 Port Status

This page provides current status of every port that depends on user's setting and the negotiation result.

State: Display port statuses: **disable or enable**. "Unlink" will be treated as "off".

Link Status: Down means "No Link"; Up means "Link up".

Auto Negotiation: Display the auto negotiation mode: auto/force/nway-force.

Speed status: Display 1000Mbps or 100Mbps or 10Mbps speed, port 1- 24 are 10/100Mbps, Port 25-26 are 10/100/1000Mbps.

Duplex status: Display full-duplex or half-duplex mode.

Flow Control: Display the flow control state

Full: Display the flow control is enabled or disabled in full mode.

Half: Display the backpressure is enabled or disabled in half mode.

Rate Control: Display the rate control setting.

Ingress: Display the port effective ingress rate of user setting.

Egress: Display the port effective egress rate of user setting.

Port Security: Display the port security is enabled or disabled.

BSF: Display the port broadcast storm filter control is enable or disable.

Jumbo Frame: Display the jumbo frame is supported or not for the port.

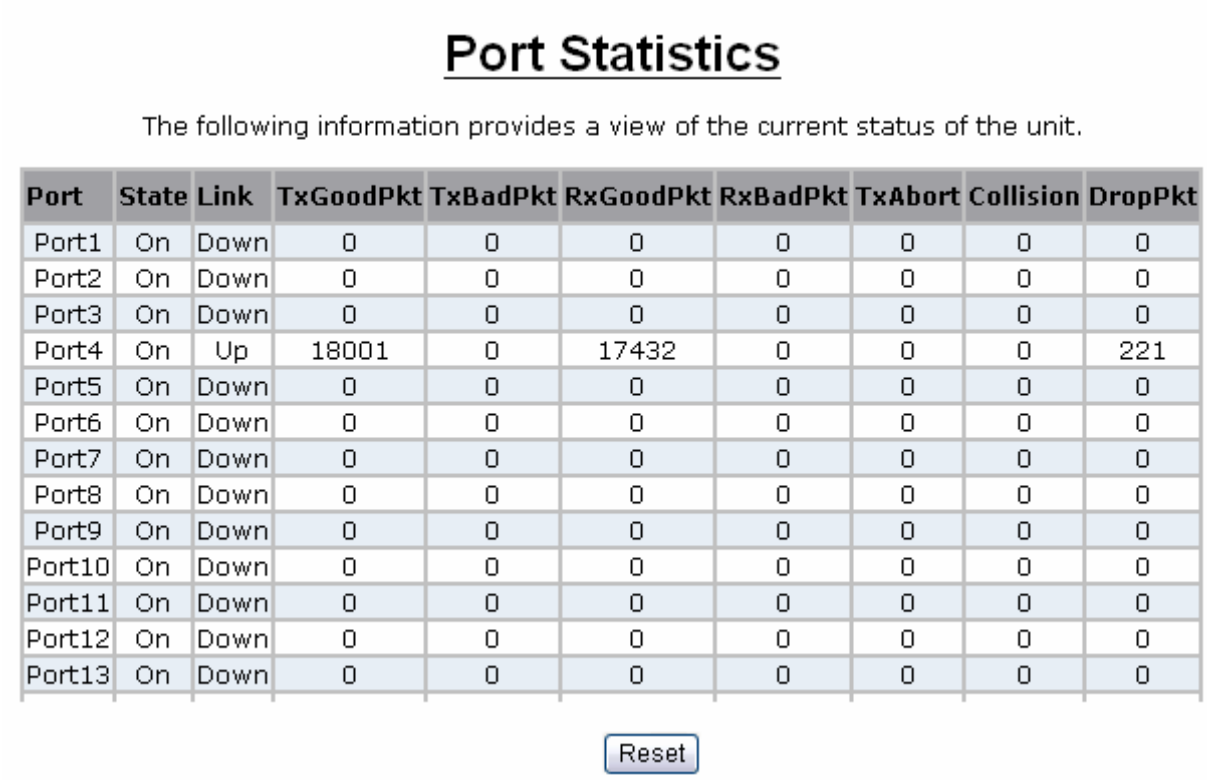
Note:

You can click the Browser's Refresh button or press <F5> to update to the latest status.

4.7.2 Port Statistics

The following information provides a view of the current status of the whole unit.

Press Reset button to clean all count.



Port Statistics

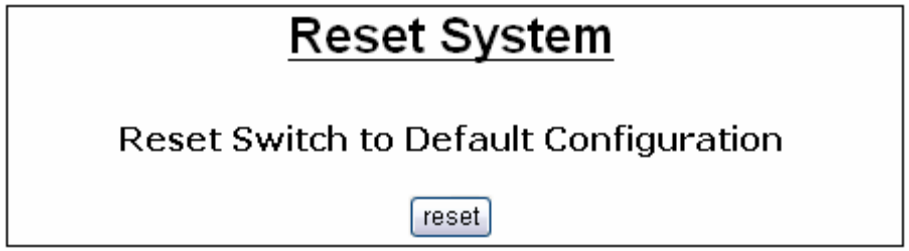
The following information provides a view of the current status of the unit.

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
Port1	On	Down	0	0	0	0	0	0	0
Port2	On	Down	0	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0	0
Port4	On	Up	18001	0	17432	0	0	0	221
Port5	On	Down	0	0	0	0	0	0	0
Port6	On	Down	0	0	0	0	0	0	0
Port7	On	Down	0	0	0	0	0	0	0
Port8	On	Down	0	0	0	0	0	0	0
Port9	On	Down	0	0	0	0	0	0	0
Port10	On	Down	0	0	0	0	0	0	0
Port11	On	Down	0	0	0	0	0	0	0
Port12	On	Down	0	0	0	0	0	0	0
Port13	On	Down	0	0	0	0	0	0	0

Reset

4.8 Reset System

The page to reset the switch to default configuration is shown as below.



4.9 Reboot

The page to reboot (warm restart) the switch is shown as below.

Chapter 5. Applications

The Switch provides segmented network architecture. When a port is connected to an end-node, or to a device that breaks up the collision domain (e.g., another switch, bridge or router), the attached device has access to the full bandwidth provided by that port.

Bridging Functions – The Switch provides fully transparent bridging functions which automatically learn node addresses, which are subsequently used to filter and forward all traffic based on the destination address. When traffic passes between devices attached to the same shared collision domain, those packets are filtered from the switch. But when traffic must be passed between unique segments (i.e., different ports on the switch), a temporary link is set up between the switch ports which need to pass this traffic, via the high-speed switching fabric.

Flexible Configuration–This Switch is not only designed to segment your network, but also to provide a wide range of options in setting up network connections. It can be used as a simple stand-alone switch; or can be connected with standard hub, switches, or other network interconnection devices in various configurations. Some of the common applications for the Switch are described in this chapter.

Switch Used as Collapsed Backbone for Starter Network

This Switch is an excellent choice for new Ethernet installations where significant growth is expected in the near future. You can easily build on this basic configuration, adding direct full-duplex connections to workstations or servers (i.e., up to 20 Mbps or even 200 Mbps of dedicated bandwidth per node).Then, when the time comes for further expansion, just daisy-chain any IEEE 802.3 or IEEE 802.3u compliant switch or hub. This Switch can also be easily integrated with upper-level protocol devices you later add into the network.

Used as apartment for Internet access

The 24+2G Intelligent Ethernet Switch provides a high speed, 10/100Mbps transmission over Ethernet wiring over a single Internet account to provide simultaneous independent Internet access to multiple users.

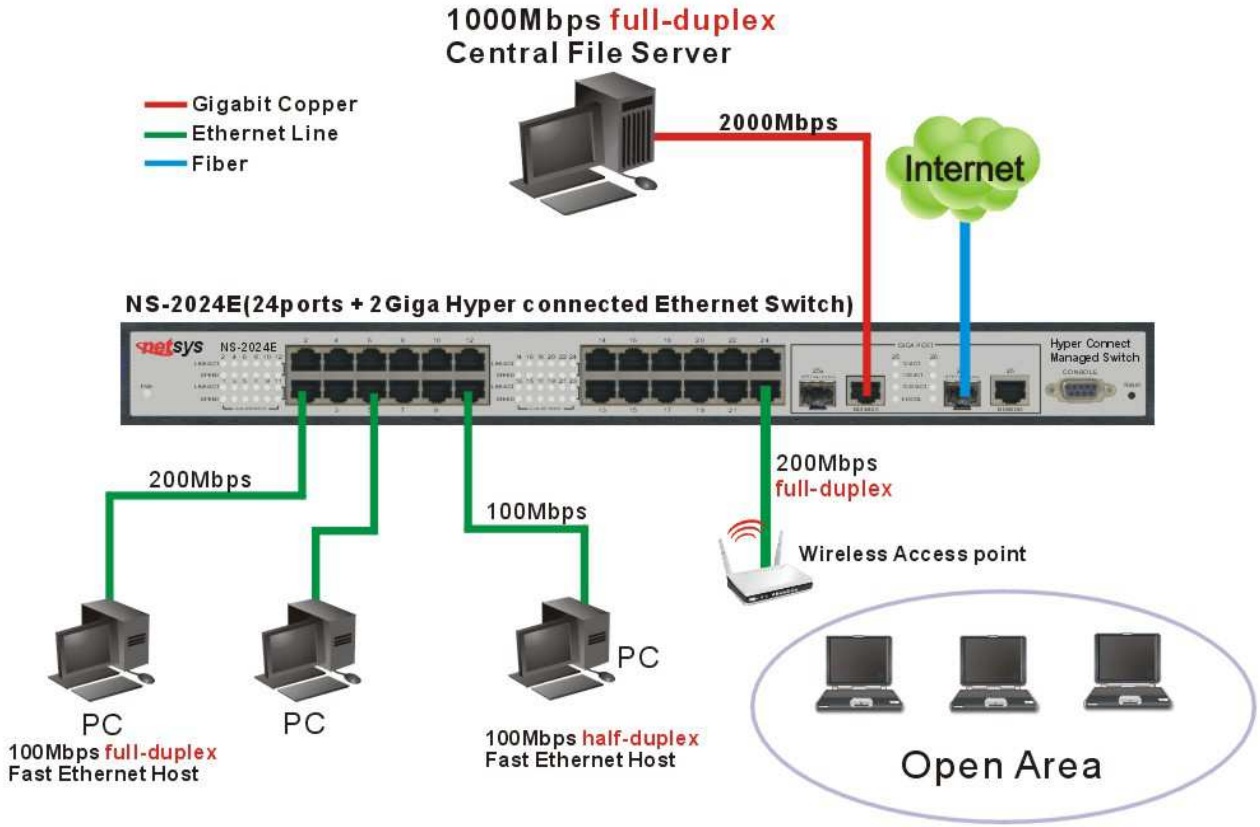


Figure 4.1 Ethernet Switch Application

Application for Sharing a single internet account

If multiple users would like to share a single internet account using the switch, which is to be connected to a IP sharing device, then to a xDSL or Cable Modem.

Note:

For network applications that actually require
Router (e.g., Interconnecting dissimilar network types), attaching the SWITCH directly to a router can significantly improve overall home networking performance.

High bandwidth backbone ready

The 24+2G Intelligent Ethernet Switch provides 10/100/1000Mbps auto sensing for external trunk device (Fiber optics, Wireless Bridge, xDSL & other WAN services).

Multi-port Bridge with High-Bandwidth Backbone

Most networks are interconnected with traditional 2-port bridges that insert significant latency into normal communications. For traffic that must pass through several bridges to reach its destination, this latency can considerably degrade communications. With 10 parallel bridging ports (i.e., 10 distinct collision domains), the Switch can collapse a complex network down into a single efficient bridged node, increasing overall bandwidth and throughput. Segments attached to the Switch no longer have to cross the backbone, now reaching each other at near-zero latency. However, for high-bandwidth applications that must pass data across the network backbone, the 24 ports can provide a high-speed remote uplink for fast access.

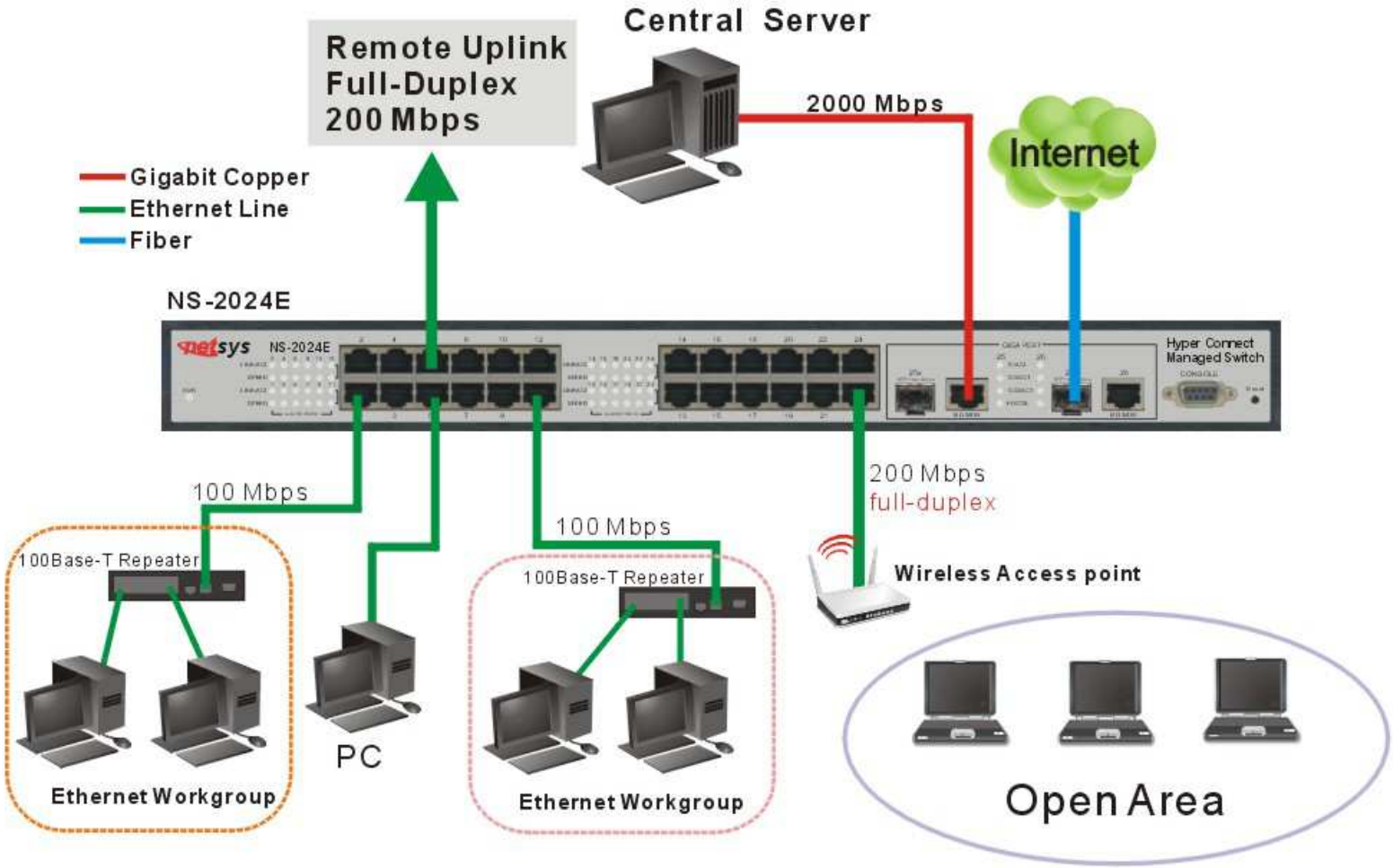


Figure 4.2 Ethernet Switch Application 2

Appendix A: Troubleshooting

Diagnosing Switch Indicators

The Switch can be easily monitored through its comprehensive panel indicators. These indicators assist the network manager in identifying problems the Switch may encounter. This section describes common problems you may encounter and possible solutions

1. Symptom:	POWER indicator does not light up (green) after power on.
Cause:	Defective power outlet, power cord, internal power supply
Solution:	◆ Cheek the power outlet by plugging in another that is functioning properly. ◆ Check the power cord with another device. If these measures fail to resolve the problem, have the unit power supply replaced by an qualified distributor.

2. Symptom:	Link indicator does not light up (green) after making a connection.
Cause:	Network interface (e.q., a network adapter card on the attached device), network cable, or switch port is defective.
Solution:	2.1 Verify if both of the switch and attached device are powered on. 2.2 Be sure the cable is plugged into both the switch and corresponding device. 2.3 Verify that the proper cable type is used and its length does not exceed specified limits. 2.4 Check the adapter on the attached device and cable connections for possible defects. 2.5 Replace the defective adapter or cable if necessary.

3. Symptom:	Upstream bandwidth control failed.
Cause:	NIC(Networking Interface Card) does not have flow control function.
Solution:	Be sure the NIC(**Networking Interface Card**) supports flow control function.

4. Question:	Right now, we've got some problem with an incorrect system password setting. How can we do a system password recover of your NS-2024E product? It's possible to made a system reset or to upload a new firmware?
Answer:	Run Hyper terminal into terminal window and setup step are as follow: 1. Please connects NS-2024E's console port to PC or Notebook PC series port. 2. Launch "Hyper Terminal" into terminal window. 3. Power on NS-2024E and wait some times until show login menu. 4. Set "Bits per second" at 115200 to the content window. 5. Set "Flow control" at None. Please see attached file to config port settings. 6. Connects PC with the NS-2024E, you will find login manual window on the screen then enter Login name ："**hsichih**" ; password："**netsys**" (Engineer user name and password) 7. Enter the "**default**" let NS-2024E reset configurations to default. 8. Enter the "**reboot**" to reboot the NS-2024E 9. Please enter login name ："**admin**" ; password："**123**" to access configuration menu.
Note:	The "reset to default" process will modify all of the configuration to default.

5. Question:	The customer reported that bandwidth control did not work in either direction when the port was set to 1 on the ingress and 1 on the egress. One of our new HP laptops should bandwidth control at around 100K on the download, but around 1.7Mbps on the upload. On my laptop, it was around 100K on the download and 225K on the upload. Is there a reason why we are seeing such varied results and has there been any other reported problem with this feature lately?
Answer:	Regarding our NS-2024E' principle of bandwidth control, which must rely on flow control to limit bandwidth over hardware, as long as client side doesn't support flow control, the upstream bandwidth control is invalid, so for this case, client side must support flow control function.

System Diagnosis

Power and Cooling Problems

If the POWER indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply as explained in the previous section. However, if the unit should turn itself off after running for a while, check for loose power connections, power losses or surges at the power outlet, and verify that the fan on back of the unit is unobstructed and running prior to shutdown. If you still cannot isolate the problem, then the internal power supply may be defective. In this case, contact your supplier for assistance.

Installation

Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (e.g., the power cord or network cabling), test them in an alternate environment where you are sure that all the other components are functioning properly.

Transmission Mode

The default methods of selecting the transmission mode for all RJ-45 ports are auto-negotiation. Therefore, if the Link signal is disrupted (e.g., by unplugging the network cable and plugging it back in again, or by resetting the power), the port will try to reestablish communications with the attached device via auto-negotiation. If auto-negotiation fails, then communications are set to half duplex by default. Based on this type of industry-standard connection policy, if you are using a full-duplex device that does not support auto-negotiation, communications can be easily lost (i.e., reset to the wrong mode) whenever the attached device is reset or experiences a power fluctuation. The best way to resolve this problem is to upgrade these devices to versions which support auto-negotiation.

Cabling

1. Verify that the cable type is correct. Be sure RJ-45 cable connectors are securely seated in the required ports. Use 100Ω straight-through cables for all standard connections. Use Category 5e-7 UTP/STP for 10/100/1000Mbps, Category 5 UTP/STP for 10/100Mbps and Category 3,4 UTP for 10Mbps Ethernet connections.
2. Make sure all devices are connected to the network. Equipment any have been unintentionally disconnected from the network.
3. When cascading two devices using RJ-45 station ports at both ends of the cable (i.e., an Auto-MDIX port), if supports a auto-MDIX used, crossover cable is not need.

External Adapters

Make sure the network interface hardware and software drivers for the attached devices are functioning properly. Check the adapter cards and associated drivers used in any attached workstation or server.

Physical Configuration

If problems occur after altering the network configuration, restore the original connections, and try to track the problem down by implementing the new changes, one step at a time. Ensure that cable distances and other physical aspects of the installation do not exceed recommendations

System Integrity

As a last resort verify the switch integrity with a power-on reset. Turn the power to the switch off and then on several times. If the problem still persists and you have completed all the preceding diagnoses, contact your dealer for assistance.

FCC Warning

This equipment has been tested to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment can generate, use, and radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at owner's expense.

CE Mark Warning

This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Warranty

The original owner that the product delivered in this package will be free from defects in material and workmanship for one year parts after purchase.

There will be a minimal charge to replace consumable components, such as fuses, power transformers, and mechanical cooling devices. The warranty will not apply to any products which have been subjected to any misuse, neglect or accidental damage, or which contain defects which are in any way attributable to improper installation or to alteration or repairs made or performed by any person not under control of the original owner.

The above warranty is in lieu of any other warranty, whether express, implied, or statutory, including but not limited to any warranty of merchantability, fitness for a particular purpose, or any warranty arising out of any proposal, specification, or sample. Shall not be liable for incidental or consequential damages. We neither assumes nor authorizes any person to assume for it any other liability.

Note: Please do not tear off or remove the warranty sticker as shown, otherwise the warranty will be void.

Chinese SJ/T 11364-2006

部件名称	有毒有害物质或元素					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬[Cr(VI)]	多溴联苯(PBB)	多溴二苯醚(PBDE)
结构壳体	○	○	○	○	○	○
电路组	○	○	○	○	○	○
电源供应器	○	○	○	○	○	○
风扇	○	○	○	○	○	○
线材	○	○	○	○	○	○
包装及配件	○	○	○	○	○	○

○：表示该有毒物质在该部件所有均质材料中的含量均在 SJ/T 11364/2006 标准规定的限量要求以下。

╳：表示该有毒物质至少在该部件的某依均质材料中的含量超出 SJ/T 11364-2006 标准规定的限量要求。

上述规范仅适用於中国法律